CyBOK

Assessing the cross-disciplinary accessibility of CyBOK

Dr Xavier Carpent and Prof. Steven Furnell

School of Computer Science
University of Nottingham

June 2023

Table of Contents

1 Introduction

This report presents the activity and outcomes of a CyBOK-funded mini-project that was proposed to investigate the accessibility of the current CyBOK resource to participants coming from outside the cyber security sector. The project ran from September 2022 to May 2023, and was undertaken by the academic investigators from the University of Nottingham, with support and oversight from Prof. Andrew Martin and Helen Jones in the CyBOK project team.

1.1 Context and Motivation

Cyber security is typically associated with computer science and IT as its primary parent discipline. However, it is clearly relevant to a wider audience and regularly draws upon other discipline areas. As such, it can be interesting and valuable to investigate the extent to which CyBOK can act as a meaningful reference point for participants coming from outside the computing / computer science discipline area. For example, within the current CyBOK structure the *Law & Regulation* Knowledge Area (KA) has clear potential to speak to practitioners from that discipline, and at least some aspects of the wider KAs from the *Human, Organisational and Regulatory Aspects* domain will be relatable to practitioners from business (e.g. *Risk Management & Governance*) and psychology (e.g. *Human Factors*). Across the wider set of KAs, many are clearly going to be relevant to in cross-sector contexts, but it is less clear whether practitioners from those sectors would find them relatable.

The primary benefit of the project is the exposure of CyBOK to a wider interdisciplinary community and insight into their ability to interact with it. The work could form a foundation for the notion of a CyBOK "Sector Lens", allowing alternate views of CyBOK to be established that are geared towards supporting better understanding for participants in different sectors, framed in a manner that speaks from their discipline rather than being computing-led.

It is important to preface that CyBOK was not necessarily designed for a non-expert / non-IT audience, and this project investigates how it is currently (or could in theory be) perceived/used by non-experts. The comments and insights that result from this investigation are therefore to be understood with this perspective in mind.

1.2 Project Structure

The project involved participants from various backgrounds in two activities: a web-based survey, and a series of online workshops, and was divided in two phases.

In phase I, the survey was used to establish the participants' perception of cyber security, and what is relevant in the context of their discipline/sector (in terms of identifying where their discipline has a need for cyber security as well as any aspects in which they feel it contributes towards achieving it). The activity involved capturing key words and phrases (KWoPs) from the participants, and their level of familiarity and perceived relevance of CyBOK's various KAs. Identified KWoPs were used to determine the extent to which these may be mapped to current KAs using the existing CyBOK Mapping Reference.

In phase II, workshops were organised with subsets of participants grouped by sectors. Elements of the CyBOK content identified through mapping the relevant KWoPs were presented back to the participants, in order to then determine whether the material covers the expected aspects, whether the presentation (e.g. phrasing and level of content) is meaningful, and/or the extent to which content would need to be reframed to make it accessible.

2 Online Survey

The first phase of data collection for the project was based upon an online survey, with the aim of getting some initial inputs from representatives from a variety of sectors.

2.1 Survey Design and Rationale

The aim of the survey was two-fold:

(1) to gain insight into the extent to which respondents from non-cyber / IT sectors are able to relate to CyBOK; and

(2) to have a means of identifying KWoPs that could then be mapped to CyBOK and form a basis for discussion in follow-on workshops.

Given that the survey context did not offer a basis from which to enable respondents to properly *make use* of CyBOK, we sought to engineer a context that would nonetheless enable us to obtain KWoPs that could then be used as a basis for reference later. The approach could then be considered broadly similar to a use case in which people may attempt to make use of CyBOK in order to further their understanding of security concepts (e.g. by looking for definitions and background information in relation to keywords or issues that they may have heard of). This also represents a task for which it can be reasonably assumed that CyBOK 'users' from other discipline areas would *expect* to be able to use it.

With the above in mind, the main question included from which to obtain KWoPs was:

- List any keywords or phrases that you associate with the cyber security needs of your organisation.

Recognising that there would likely be a limit to the number of KWoPs that respondents would identify in response to a single question, this was further supplemented by two additional questions as an opportunity to extract further thoughts:

- List any other keywords or phrases that you associated with cyber security as a topic.
- Identify any topics that you feel that your sector contributes to cyber security.

All three questions invited free text responses, with the boxes themselves being large enough not to limit the extent of the replies. Note that these questions were all asked *prior* to presenting the respondents with any headings or other content from CyBOK itself, as we did not want this to influence their responses.

Having identified the KWoPs, the remainder of the survey was focused around understanding and appreciation of the 21 CyBOK Knowledge Areas. This was achieved via two more substantial questions as follows:

1. Indicate your understanding of the different CyBOK Knowledge Areas
2. Indicate your perception of the relevance of each Knowledge Area to your organisation.

For these tasks, each of the KAs was presented by means of its name and the accompanying outline description from the CyBOK Tabular Representation.

2.2 Survey dissemination

In terms of eligibility to participate, respondents were required to be 18 years or over, and to be regular users of IT in the context of their workplace. Amazon vouchers worth 15GBP were offered as an incentive for participation, and ethics approval for the activity was obtained from the School of Computer Science Research Ethics Committee (CS REC) at the University of Nottingham prior to commencement of any data collection (application ID CS-2022-R23). Note that the same ethics application also covered the conduct of the later workshops, for which the incentivisation payment was increased to 30GBP in recognition of the greater time commitment.

The survey was conducted in a phased approach over a period of 3 months, using a set of initial contacts in different sectors as a means of promoting the questionnaire to further relevant participants. In line with the original project proposal, the target was to achieve 30 participants across a range of sectors, with the upper threshold being set by the number of vouchers available. In practice, it took longer than anticipated to meet the target sample, as we realised that each time an attempt was made to promote the survey via a contact point, time then needed to be allowed to pass to determine whether responses were received before then following up or approaching an alternative contact. We could not approach multiple promotors for the same sector in parallel for fear of then having too many responses from one area and reducing the supply of vouchers for others.

We also elected to get a reference sample from a small number of participants from the cyber sector, in order to determine how their responses compared to those from the respondents more generally.

The questionnaire was implemented and distributed via the SurveyMonkey service, and a full copy of the resulting material can be found in Appendix A.

2.3 Findings

A total of 33 participants from various backgrounds completed the survey, as summarised in Table 1. This is considered to represent a suitable sample to work with from a range of distinct areas, as well as having a suitable basis to contrast the cyber and non-cyber responses in later questions. It should be noted that the response from the DCI sector was not one that had been specifically sought, and so does not receive any specific attention in the analysis, but is included in the broad group of ‘non-cyber’ responses when comparing against the cyber sector.

Sector	Responses
Cyber	5
Design and Creative Industries	1
Education	5
Finance and Insurance	5
Healthcare	3
Government	4
Law	5
Policing	5
Total	**33**

Table 1 : Summary of survey respondents by sector

The average completion time, as reported by SurveyMonkey, was 13 minutes. Overall, 70% of the respondents were male and the remaining 30% female. In terms of levels of experience in their respective sector, the overall results are presented in Figure 1.

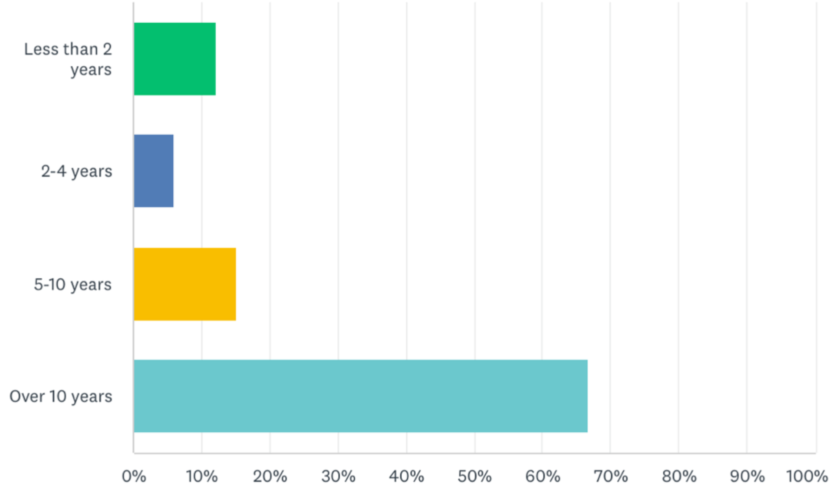


Figure 1 : Respondents' years of work experience in their respective sector

Respondents were also asked to rate their familiarity with IT and cyber security, and the results are depicted in Figure 2. Unsurprisingly, the majority of the 'Extremely familiar' responses come from the cyber sector respondents, all but one of whom rated themselves at this level for both aspects (in the other case they rated themselves 'somewhat familiar' with IT and 'very familiar' with cyber security).

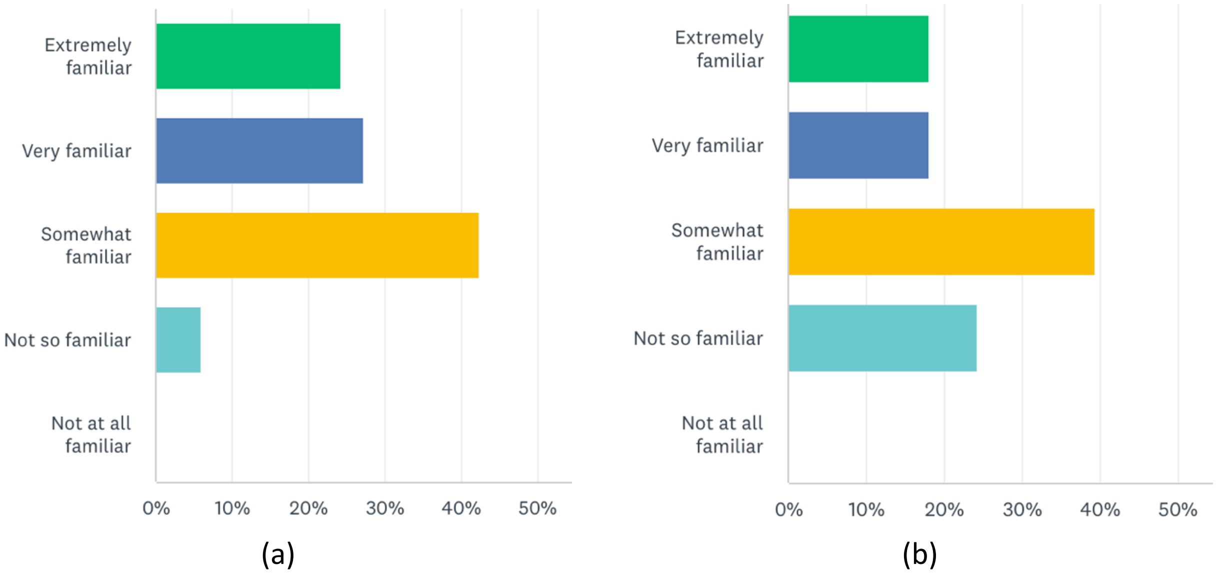


Figure 2 : Self-declared familiarity with (a) IT and (b) cyber security

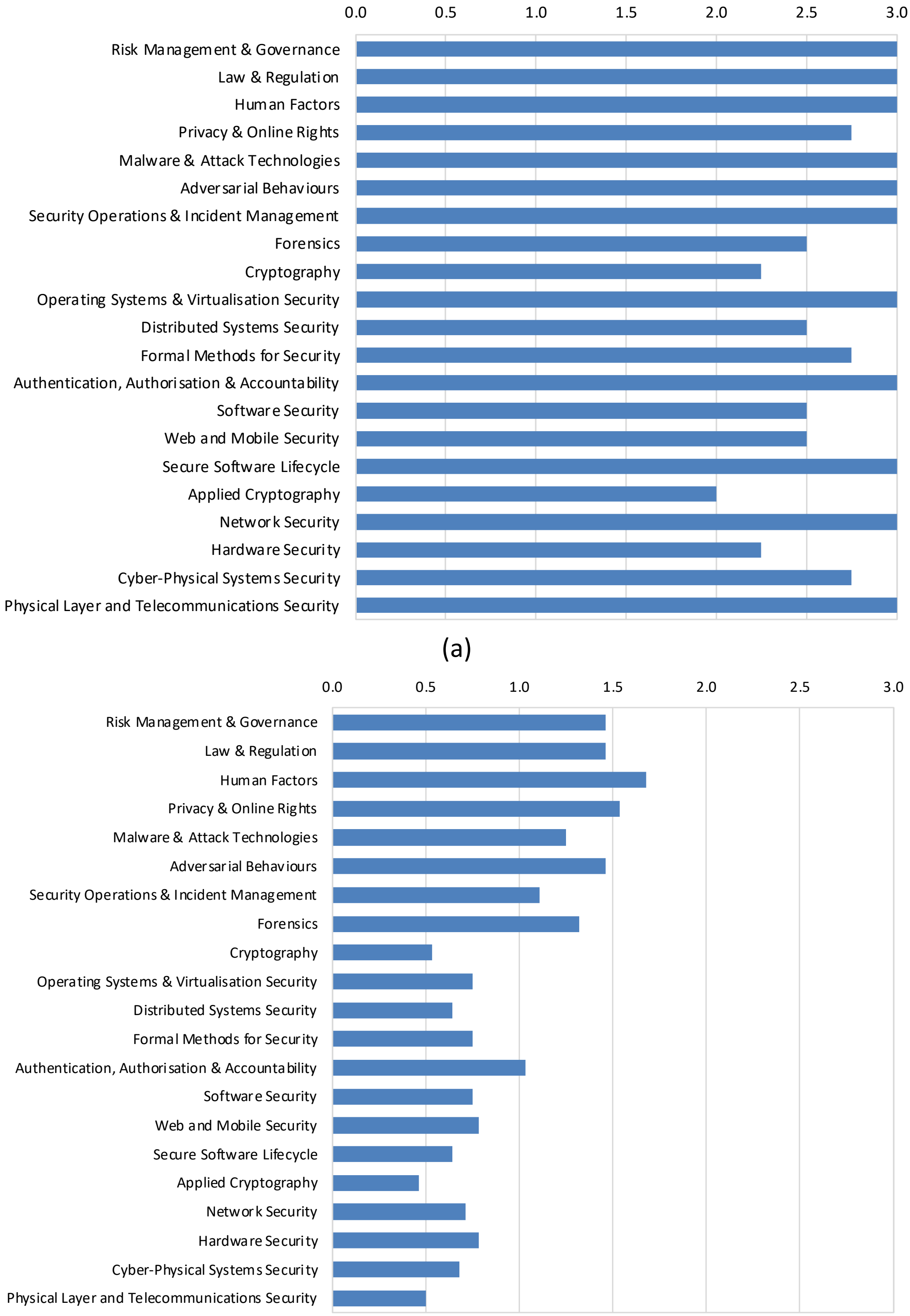
The KWoPs identified in each response were collected, partitioned into various sectors, and were used to select material for the subsequent workshop.

The remaining part of the survey, and potentially the more time-consuming aspect, asked the respondents to consider each of the CyBOK Knowledge Areas, and rate their level of understanding based on the following levels:

- I have no understanding (0)
- I have a little understanding (1)
- I have a reasonable understanding (2)
- I have a good understanding (3)

As a basis for gauging their understanding, each KA entry included its full title and the brief 1-2 sentence description of it offered by the CyBOK Tabular Representation. These descriptions were presented directly in the survey (as opposed to asking respondents to link to them or look them up elsewhere) and were chosen on the basis that they are brief and were written as a plain language indicator of what each KA seeks to address.

The average scores resulting from these assessments are presented in Figure 3, illustrating the significant difference in the average understanding claimed by the set of cyber sector respondents versus the 27 from other sectors. While this is arguably unsurprising on one level, it nonetheless indicates that even the simplified descriptions in the Tabular Representation are not coming across clearly in many cases. It is notable that there is a somewhat better level of claimed understanding across the KAs from the *Human, Organisational and Regulatory Aspects* category than from the other four (more technically-focused) categories.



(a)

(b)

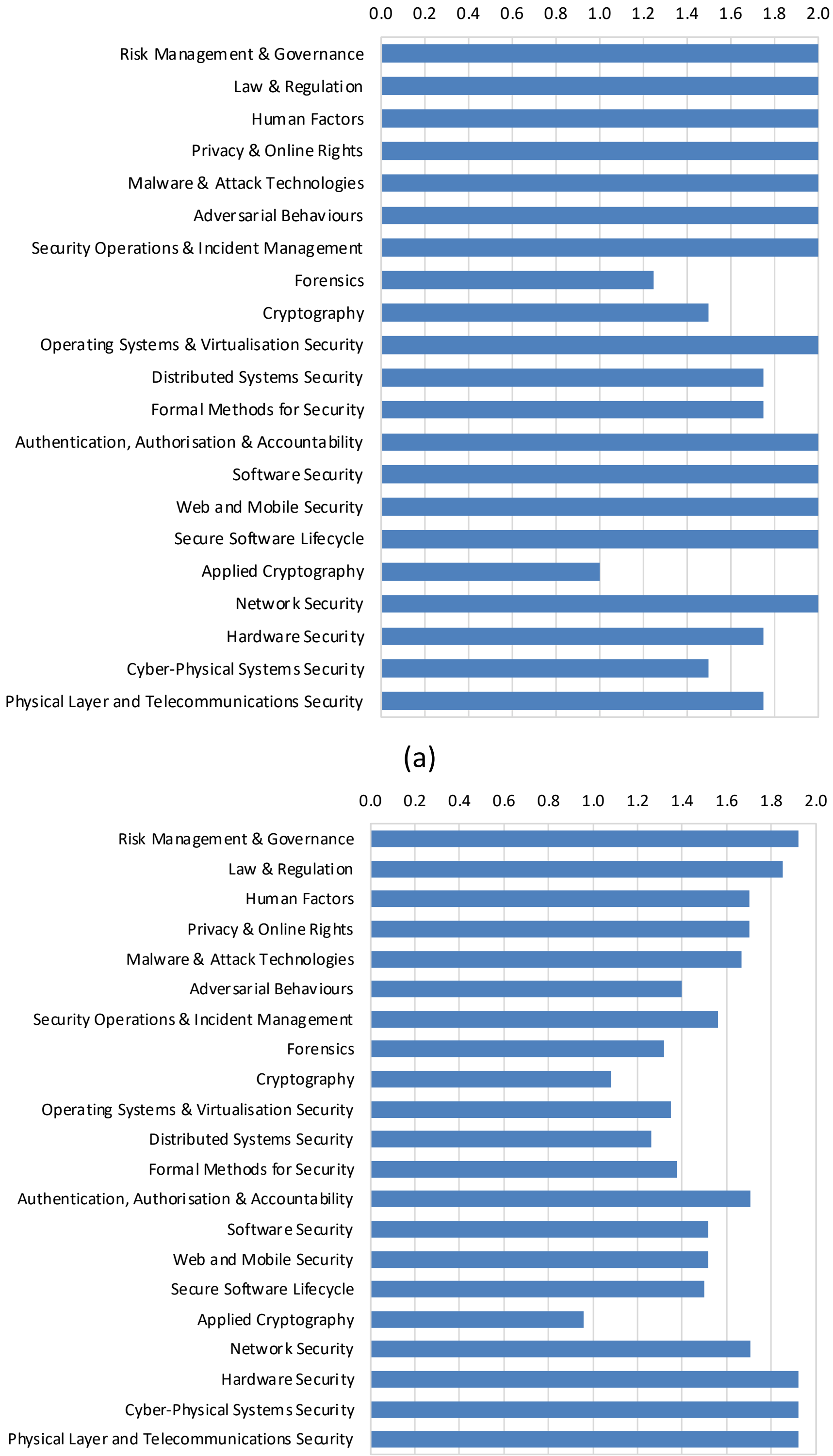
Figure 3 : Understanding of Knowledge Areas in (a) cyber sector and (b) other sectors

The next question retained the focus on the KAs, but now asked the respondents if they considered the KAs relevant to the needs of their organisation. The ratings in this case were at three levels, plus an option for 'Don't Know':

- Not relevant (0)
- Somewhat relevant (1)
- Very relevant (2)

The results are shown in Figure 4, noting that there is not such a dramatic difference now between the cyber and non-cyber respondents (although the latter group's answers also had 13% of Don't Know responses, whereas there were none from the cyber respondents). What this would appear to suggest is that although they do not fully understand what the different elements of cyber security may *mean*, the respondents from non-cyber backgrounds are nonetheless very willing to accept that they are relevant to their organisation in some way.

The final section of the survey was optional and invited respondents to offer any additional thoughts or expand upon their earlier responses. Most elected not to do so, but those that did are presented in Table 2 (given that there were a limited number, the quotes are presented in full). Where there are multiple quotes from the same sector, they are coming from different respondents.



(b)

Figure 4 : Perceived relevance of Knowledge Areas in (a) cyber sector and (b) other sectors

Sector	Respondents’ comments
Cyber	“Not explicitly mentioned above " secure by design" ,"Privacy by Design". Security Tooling . Secure infrastructure life cycle. Vulnerability management , Security assurance and audit. Supply chain.”
Education	“Generally rely on IT department to lead development in this area, however, going through the questions, as administrators of systems & data, there feels a gap in understanding of this area given the significant impacts of any breach etc.” “I think all information is relevant to an extent to as it increases awareness, not only to users but also makes people stop and think and look at ways we could improve cyber security.”
Financial and insurance	“I understand my own role very well but most of the above is in a language I don't completely understand. I rely on the cyber-security team within my organisation to tell me what I need to know (which I am confident they do)”
Government	“As an organisation with a public delivery duty and an extensive digital footprint across a mix of mediums and platforms, we have extensive knowledge around cybersecurity and management internally. Knowledge is however often heavily segmented to digital lead, platform and service owners, dependent on role and duties. Hence the mismatch between personal expertise and need above. In many ways, knowledge about wider cyber security and specialist functions has tended to come from professional curiosity and interest rather then an active attempt to train people outside of digital functional areas across the public sector. I would say that day to knowledge across non specialist staff is pretty limited at times.”
Healthcare	“Lots of terms that I am not familiar with. Hoping there are those in my organisation who do this work to keep my work safe.” “never heard of cryptography”
Law	“I find the technical language very difficult as I am not technically adept. I feel that, like most technical subject areas, 'dumbing down' is crucial for understanding, but is very difficult for those with a high level of technical knowledge. Description by analogy is the most useful technique for me (for example describing an IT system with reference to an everyday system such as central heating or how a car works or a conveyor belt in a factory, or something like that). I understand the risks in general of data becoming compromised, lost or stolen, but the best way to get across the risks is to give real (or even realistic) examples of cyber security issues that have happened/are likely to happen, as that tends to be sufficiently terrifying to prompt close attention!”
Policing	“As working in Policing, cyber security is always going to be very important as a sector, however there will be a massively broad range of knowledge required. That being said, the overall knowledge of cyber security across the force would be considered low and should be much higher.”

Table 2 : Free-text comments from survey respondents

3 Workshops

The workshops were designed as a means to collect more specific insights from the participants. Using the information gathered in the survey phase, the key question posed by the workshops was essentially if the participants' chosen KWoPs were to be used as their route into further exploration of cyber security, to what extent does CyBOK support them in furthering their journey?

Participants were grouped according to their professional sector, and (when possible) a workshop was organised for a selection of sectors where a sufficient number of participants were present and willing. A total of 4 workshops were held: Law, Education, Emergency Services, and Cyber sector. As previously mentioned, the latter was mostly used as a baseline to put the non-expert workshops in perspective, but the discussion that emerged may be independently considered insightful.

The discussions in the workshops helped to confirm that looking for definitions was a valid use case – people outside the cyber or IT sectors need these as a way into the topic, and so if they are terms that they already associated with cyber security then it is relevant to consider what CyBOK has to say about them.

3.1 Recruitment and Preparation

As with the survey responses, recruitment and scheduling of the workshops proved more challenging than originally anticipated. Despite various survey respondents having indicated that they were willing to participate in a follow-up workshop, it then proved difficult to get several of them to respond to resulting emails to invite them. There was then a further challenge in terms of scheduling sessions on suitable date/timeslots for those people that did respond. In the end, four workshops were scheduled, but most only managed to secure three participants on the day. As can be seen from Table 3, the workshops were scheduled over a period of three months, with attempts to schedule them only being possible once a threshold number of survey responses had been received for the sector concerned. In addition to those listed, attempts were made to schedule workshops for Healthcare and Government respondents, but these were ultimately aborted due to lack of responses and/or availability issues. Note that in the Table, the 'Emergency Services' session was an amalgamation of respondents that had replied from the Policing group and one from the Government group who actually worked for the fire service.

Workshop Date	Sector	Invitees	Participants	Duration
17 February	Law	4	3	59m
4 April	Education	4	3	57m
4 May	Cyber	4	4	1hr 17m
15 May	Emergency Services	5	3	57m

Table 3 : Summary of Workshop sessions

3.2 Workshop preparation

In advance of each workshop, the KWoPs identified in the survey were collated and, for each KWoP that appeared at least twice (for removing outliers and focusing the discussion on commonalities) we undertook the following process:

1. Use the CyBOK Mapping Reference and find the KWoP (or the term(s) most closely related);
2. Select the most appropriate KA(s);
3. Search the relevant KA(s) for sections of text where the KWoP is *defined* or *introduced*.

This arguably corresponds to what a non-expert desiring to use CyBOK to learn about a topic would wish to do with the material presented to them. The text(s) identified in Step 3 were then presented to the participants during the workshop (5 to 8 excerpts in each workshop).

We point out that none of the above steps were particularly straightforward for us:

- KWoPs did not always appear directly in the Mapping Reference, and some educated guesses were sometimes necessary;
- Conversely, KWoPs sometimes matched many entries, which in turn mapped to many KAs;
- Selecting the most appropriate KA (possibly among many) was not always straightforward;
- Finding where a KWoP is first introduced within a KA is inconsistent.

There was therefore a degree of interpretation on our part. From there, as best we could, we then extracted material that best *defined* or *introduced* each selected KWoP, and used these as a basis for discussion during the workshops. Table 4 summarises the KWoPs that were presented to participants in the four workshops, with the KA(s) that they were sourced from. The associated text experts used for each KWoP from each KA are presented in Appendix C.

KWoP	Source KA(s)	Workshop			
		Cyber	Education	Emergency Services	Law
Awareness	HF		✓		
Business Continuity	RMG, SOIM	✓			
Data Protection	LR	✓			✓
Denial of Service	NS, AB			✓	
Firewall	NS	✓		✓	
GDPR	LR		✓		
Passwords	AAA, WAM	✓		✓	✓
Penetration Testing	SSL	✓			
Phishing	AB	✓	✓	✓	
Protection	CPS, HS, CI		✓		
Ransomware	AB	✓	✓	✓	✓
Secure Email	NS				✓
VPN	NS			✓	

Table 4 : Summary of KWoPs presented in the different Workshop sessions

3.3 Workshop Sessions

As previously indicated in Table 3, most workshops lasted around an hour, and followed a similar structure:

1. Recap of the project and rationale;
2. Background about CyBOK, the Mapping Reference, the KAs, and the Tabular Representation;
3. Survey Findings (for that particular group/sector);
4. KWoPs and excerpts selection process;
5. Discussion about excerpts, and final thoughts.

Steps 1-4 tended to take around 15 minutes in total, allowing the majority of the session time for the discussion. This last step was where participants would mostly be active, and was the longest by far (~40min). The material was presented on the screen, participants were given time to read it, and then invited to take turns and voice their opinions. The discussion was centred around the following questions:

- Does the material cover expected aspects?
- Is the presentation (e.g. phrasing, level of content) meaningful?
- How would the content need to be reframed to make it more accessible (to you)?

An example of the slide materials used to support the workshops is provided in Appendix B.

3.4.1 Law Sector

There were three participants from the law sector in this workshop. Below is a list containing all KWoPs identified in the relevant surveys. KWoPs that appear twice or more are presented in bold.

Survey question	Merged responses from Law respondents
Please list any keywords or phrases that you associate with cyber security needs of your organisation	**Encryption**. **Password**. Confidential. **Data Protection**. Secure Backup **Hacking** **Data Protection** Privacy Sensitivity of data **Data protection** Personal information **Encryption** VPN Remote access Shared drive access **Password** Secured Drive Redaction of documents **Secure e-mail** accounts **Passwords**, passcodes, dual authentication, **secure email**
Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation?	Fraud Identity theft Stealing data Phishing **Hacking** Intercepted communications (written and oral) **Ransomware** attacks Data **breach**, cyber attack, **ransom ware**, malware
Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security?	Regulation. **Enforcement** Not sure Education on legal liability for cyber security **breaches**. Education on minimisation of risk of exposure to legal liability for cyber security **breaches**. **Data protection** legislation education My sector deals with the **enforcement** / sanctions imposed on people who commit cyber security **breaches** offences

Table 5 : KWoPs identified by Law sector respondents

Among the KWoPs in bold, those chosen for the workshop were Data Protection (LR), Passwords (AAA, WAM), Ransomware (AB), and Secure Email (NS).

Below is a compilation of comments that the participants made during the discussions, for the different excerpts.

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
Data protection	LR	• quite a good intro • need to reach police/enforcement; maybe not good for that • by a lawyer, for a lawyer • terse • if not for a lawyer, not any good • learning by example	Overall a positive reaction, with the recurring comment that the material is "terse", and in this case difficult to read for non-lawyers. As it will become clear with the other workshops, the "learning by example/illustrations" comment is also frequent. Note that there is a notable bias here, with the audience being quite comfortable with the specific topic.
Passwords	AAA WAM	• first and final paragraph [from AAA version] not clear • lacking examples again; what is meant practically • the excerpt from web and mobile security is a lot better as an introduction [than that of AAA]	Unsurprisingly, participants are often lost when the material becomes technical, such as here when discussing hashing, salting, shadow files, etc. This is particularly the case with unfamiliar acronyms (RADIUS, DIAMETER, etc.). Interestingly, the excerpt from WAM seem to have been much better received than the excerpt from AAA.
Ransomware	AB	• very good • lacking a bit of framing (couple sentences in the beginning)	Of note here is that the inclusion of numbers and examples resonated with the participants.
Secure Email	NS	• unclear who the audience is? • too much tech info • starts off well, then becomes too technical • why is it secure? what does it mean?	Participants were struggling here again with acronyms, and with the relative technical level of the text. This particular instance arguably required a fair amount of technical background to make sense of.

Table 6 : KWoPs discussed in Law sector workshop and comments arising

Wrapping up the workshop, participants were asked for global comments, particularly regarding what would make these texts more approachable/useful to them.

Comments focused on the technical nature of much of what was presented to them. Non-experts seem to resonate particularly well with examples, numbers, consequences of non-compliance, etc.

Participants also floated the idea of involving non-experts in the writing process, to guarantee the accessibility of the text, to split text in non-technical and technical parts, and/or to provide a glossary of terms.

3.4.2 Education Sector

There were three participants from the Education sector in this workshop. Below is a list containing all KWoPs identified in the relevant surveys. KWoPs that appear twice or more are presented in bold.

Survey question	Merged responses from Education respondents
Please list any keywords or phrases that you associate with cyber security needs of your organisation	Multi factor authenticity , VPN, Spam, data security, student data, password, authentication, **GDPR**, firewall, reputation management, Risk, reduce the risk, devices, security, malicious, **protection**, **awareness**, unauthorised use or information, NCSC, digital attacks, data, detect, **threats**, **awareness**, Online, Internet, IT, Surfing, **Protection**, Safety, IP, **GDPR**, Storage, Cloud, Safe Keeping, Vulnerability, **GDPR**, Data Protection, Breach
Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation?	**Ransomware**, hacking, **phishing**, spyware, **Phishing**, **threats**, **ransom**, money laundering, insurance, illegal activity, crime, Technology, Software
Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security?	Academic research, **training**, skills, partnerships, **Awareness**, **training**, associated policies to help prevent cyber security. Being in an education environment there is a large amount of exposure due to the number of people using devices and being able to log into system/servers online/remotely, Research, Innovation, Development, Recognition, Digital Literacy, **Education**, **Education**, **Awareness**

Table 7 : KWoPs identified by Education sector respondents

Among the KWoPs in bold, those chosen for the workshop were Awareness (HF), GDPR (LR), Phishing (AB), Protection (CPS, HS, Intro), and Ransomware (AB).

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
Awareness	HF	• very long, detailed • overcomplicated, got lost halfway through • could be better introduced • paragraph break would help • doesn't say what is the purpose	The text seemed perhaps too abstract/terse for the participants.
GDPR	LR	• does not spell out GDPR • "prescriptive jurisdiction and data protection" not the same as "GDPR" • legalese	Familiar struggles with legalese or overly technical text, and with acronyms.
Phishing	AB	• good text • examples • relatable • easy to connect/understand	Positive reaction overall, which is unsurprising, due to that fact that many non-technical people are still very much aware of what phishing entails.
Protection	CPS HS Intro	• CPS: not expecting to see this • HS: not very useful either; some terms not familiar (I/O, OS, etc.) • Intro: strange that it's "defined by what it's not"; is it meant to protect users or system operator?; perfectly understandable	Regarding CPS: this may be a problem due to the Mapping Reference or the way we used it. Participants did not expect to consider aspect of physical security. HS: too many unfamiliar acronms to make sense of text
Ransomware	AB	• interesting, easy to read • numbers are relatable • first paragraph and latter two have a different style • some things that make less sense: bootloader, MBR, blockchain, public-key cryptography	Similar sentiment as with the Law sector: overall positive, and issues with style heterogeneity and acronyms. Participants resonate with scenarios, examples, numbers, etc.

Table 8 : KWoPs discussed in Education sector workshop and comments arising

Finally, wrapping up the discussion, participants made a number of global comments on their experience. It seemed unclear who the target audience was. A participant asked whether CyBOK was meant to be UK-centric. Comments similar to the Law sector were also made: some texts are much more accessible (to non-experts) than others, they engage with examples a lot more than with conceptual discussions, structure could be improved (first high-level non-technical definitions, then more details), more cross-referencing, etc.

The participants were impressed that such a useful, vetted, peer-reviewed resource was available for anyone to use. At the same time, they thought the document form was rather “old-fashioned”, and questioned whether it was/should be “live” (constantly updated, etc.). They also floated the idea of an “education version” of KAs.

3.4.3 Emergency Services Sector

There were three participants from Policing and one from the Fire Service in this workshop. Below is a list containing all KWoPs identified in the relevant surveys. KWoPs that appear twice or more are presented in bold.

Survey question	Merged responses from Education respondents
Please list any keywords or phrases that you associate with cyber security needs of your organisation	Data security. Access control. Shoulder surfing. **Firewall**. Government Security Classification. Cloud security data protection Digital Security **Firewall** ISO accreditation **Virtual Private Network** Open Source, Complex, technical, closed shop, qualified, accredited, essential, lack of knowledge/skills. **Passwords**, **Firewall**, Digital Hygiene, CMA, Policy, Classification, prevent, prepare, **Firewalls**, data safety, **encryption**, **passcode**, vetting, official, sensitive, secret, Strong **Passwords**, Two Factor Authentication, **Firewalls**, Vigilance, Being Aware of **Phishing**, Being aware of what social engineering is, **Encryption**, Network Intrusion Detection Systems, **VPN**, VPN Tunnel
Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation?	**Spear fishing**. **Trojan**. **DDOS**. Bug Brute Force attack Data Breach DOS / **DDOS** Ethical hacking **Hacker** Hardware Hash Internet of Things IP address Keylogger **Malware** **Phishing** **Ransomware** Software Spoofing Spyware **Trojan** Two factor authentication **Virus** Worm, Confusing, lack of clarity, no clear training pathways, expensive, essential, Protocols, **virus**, secure, network, Network architecture, **Malware**, **Ransomware**, **DDos**, **Hacking**, Spearing, Whaling, On Path Attacks, Penetration Testing
Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security?	Limited advice to members of the public about what to watch for and how to stay safe on line. Prevent inputs to not be a victim of Cyber Crime Pursue opportunities to detect crimes, Digital Forensics, Investigations, Intelligence, Protect and Prepare strategies. prevent, prepare, awareness, Prevention, detection, advice, guidance, safeguarding, Investigation of criminal offences that are enabled by or that are wholly reliant on computers.

Table 9 : KWoPs identified by Emergency Services sector respondents

Among the KWoPs in bold, those chosen for the workshop were Denial of Service (NS, AB), Firewall (NS, Glossary), Passwords (AAA, WAM), Phishing (AB), Ransomware (AB), and VPN (NS).

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
Denial of Service	NS AB	• NS: helps, talks about countermeasures • NS: too technical, would benefit from being dumbed down a bit • NS: terms not introduced? (BGP) • NS: first paragraph: not a definition • AB: quicker to get a grip on • AB: more of a definition, with practical example • AB: relatable, spelling out acronyms	Again unsurprisingly the two KAs have a different approach, which seems to resonate differently with non-cyber people. AB tends to focus on the adversary and its motivations, and employs examples, which makes it easier to grasp for non-experts. NS on the other hand is more technical.
Firewall	NS Gloss.	• acronyms, technical terms • "gatekeeper" is a nice terminology	Technical level again. We see here that analogies or analogical terminology helps for non-experts.
Passwords	AAA WAM	• AAA: made sense; revised recommendations are interesting • AAA: a bit too technical (hashing, salting, shadow file, etc.) • WAM: easier to read, relatable • WAM: language simple (by contrast with AAA) • WAM: stating the obvious a bit	Similar reception as with the Law sector.
Phishing	AB	• useful, maybe a bit wordy but not too bad • practical examples • criminal point of view is interesting	Again, AB and its perspective and use of examples are resonating with non-experts.

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
Ransomware	AB	• useful, similar to phishing: worded on a practical level, with examples • citation a bit confusing • reads well • nice to have a comparison between ransomware and other types of fraud • interesting that it did include sources • MBR etc. not known	Same as above.
VPN	NS	• got lost a bit; other texts for intro to VPN easier to understand • understandable, but not a great definition	A bit divided here, mostly due to some people already being familiar with the term and allegedly already used to using VPNs.

Table 10 : KWoPs discussed in Emergency Services sector workshop and comments arising

The final global comments made by the participants were quite positive. They were “made aware of how much [they] don't know”. It seemed to them that the excerpts they were shown were pitched about right, if a bit too technical and not very friendly to non-practitioners. They struggled with acronyms and technical terms. Again, commenting on the heterogeneity of the accessibility, some KAs (e.g. AB) more "conversational", easier to understand.

3.4.4 Cyber Sector

There were four participants from the cyber sector in this workshop. Below is a list containing all KWoPs identified in the relevant survey responses. In this particular case there was a surprising lack of duplication between the terms being suggested amongst the different respondents, and so we aimed to draw out some terms that were common with other groups, so that there was a basis to compare how the definitions were then received by the cyber audience, plus a couple of additional more specialised KWoPs (Business Continuity and Penetration Testing) in order to see how these were mapped.

Survey question	Merged responses from Education respondents
Please list any keywords or phrases that you associate with cyber security needs of your organisation	As a Cyber Operations company we are comfortable with our organisation knowledge. Be legally compliant Be safe and secure Existential risk. **Data protection**, cyber defences, removal of legacy IT systems, patching, multifactor authentication, identity management, monitoring, logging, **penetration testing**, vulnerability scans, hardening, certification, **encryption**, **business continuity**.
Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation?	Knowledge, Do I need it?, Cost, who should I speak to. **hacking** state actor **malware ransomware** cyber-crime complicated expensive risk management culture
Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security?	We regularly give talks to groups & businesses on Cyber resilience. We still find people/businesses happy to "bury head in sand". Strategic planning Capability development. Publishing guidance, conducting research, creating new cyber security experts.

Table 11 : KWoPs identified by Cyber sector respondents

Among the KWoPs in bold, those chosen for the workshop were Data Protection (LR), Penetration Testing (SSL), Ransomware (AB), Firewall (NS, Glossary), and Passwords (AAA, WAM).

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
Data Protection	LR	• generic • high-level view • no mention of data type/metadata • regulatory lens, different from tech angle • history of law; don't care • doesn't introduce what we have to do, or my organisation • 2nd paragraph: not true, no overlap between practitioners (threats), data protection practitioners (data) • missing: subject access request, freedom of information	As will be the case for the other excerpts, the participants from the cyber sector were a lot more critical, and, unsurprisingly, a bit nitpicky about certain details. Nevertheless, there is certainly a lot to take away from these, and a lot of good points were made. The “missing” comments may or may not be factual, as the “missing” content may be presented elsewhere (despite being reminded several times, participants of the various workshops did not always internalize that the excerpts presented to them were not the whole story).
Penetration Testing	SSL	• missing social engineering • a lot of words for basic content • red/blue/purple teaming • explain this instead of OWASP etc. • NOT an exhaustive list of weaknesses; does not replace vulnerability scanning etc. • misconceptions about pentesting • unusual description of pentesting; not true that it is black box • mentions OWASP but no accreditation schemes • there are better definitions out there • web-app testing different than infrastructure testing • "often does by in-house": virtually always outsourced	Complaints about obsolete/outdated content, and some of the content was disputed. Same caveat as above regarding allegedly missing content.

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
		• white hat hackers: remove that term (per NCSC guidelines) • scope is a key component • should be much larger; really broad topic; most organizations do it all the time	
Phishing	AB	• limited to a certain type of phishing • most of the phishing we see is someone pretending to be in your organization • biased • no mention of targeted phishing • doesn't talk about the consequences of phishing (fraudulent scams, the fact that it's often a first step into an attack, etc.) • lack of scoping/motivation (why do phishing) • not enough context in terms of volume • no mention of organization culture/behaviour	Again, suggestions for adding content may be invalidated if they are mentioned in the rest of the KA, or could otherwise be considered.
Ransomware	AB	• "newest trend" -> not really • out of date • these days: double-extortion: copy of the data; blackmail org; sophisticated • not great for intro for non-tech • ransomware-as-a-service • for tech audience: principles of how it works (difference payload, bootloader) • no mention of recovery (backup first)	Similar comment here with outdated or allegedly incomplete content.

KWoP	Source KA(s)	Key points from participants	Researcher team commentary
		• no mention of business disruption	
Firewall	NS Gloss.	• very outdated (~2002?) • all firewalls are stateful these days • network firewalls, webapp/app firewalls • firewalls are ASICs • cloud not mentioned • in-line, tapped? • IDPS, integrated • zero-trust • firewalls less relevant these days	There was particular emphasis on the fact that the content of the Firewall KWoP was very out of date, and not at all in line with current practices.
Passwords	AAA WAM	• 20 years out of date • multi-factor authentication • would be more useful as a high-level presentation • pseudo-technical (salting, etc.) • disputable (e.g. most widely deployed) • complexity: not defined	And finally, again similar comments here as with the other KWoPs.

Table 12 : KWoPs discussed in Cyber sector workshop and comments arising

Given that they were included as a comparison group to the various non-cyber sector participants, the overall comments from these participants, including those in the wrap-up part of the workshop are discussed in Section 4.2 as part of the broader reflection on the project experience.

4 Discussion

This section presents some reflections on the overall project experience, and the accessibility of CyBOK to the different audiences that were addressed (noting that accessibility in this context encompasses both being able to find details about a topic of interest and then being able to understand the material that is presented as a result).

4.1 Reflections on accessibility to the non-cyber community

Based on the experiences from the survey and the accompanying workshop sessions, the accessibility experience for the non-cyber audience was mixed in terms of both *locating* material and then being able to *understand* it.

It is worth noting that the accessibility to non-cyber audiences varies depending upon the KA from which material is being drawn. In fact, this point may apply to the audience accessibility of KA content more broadly. For example, the Law sector participants commented that the text relating to Data Protection seemed to have been written for lawyers, and so they found it digestible but at the same time queried the accessibility of the text for a wider (non-law) audience. Meanwhile, they then found the use of technical terminology and acronyms in several of the other KWoPs presented to them (e.g. passwords, secure email) to be inaccessible. This highlights issue in the framing of the text, insofar as the KA texts may have been unintentionally but implicitly pitched to different audiences depending on the perspective of the author. Certainly, the clarity of the CyBOK content to the *same reader* will vary across the KAs (and sometimes within a KA) according to the perspective and style of the author and the prior knowledge that they have assumed. This is well-illustrated by the Law participants, with all of their KWoPs having been identified by the same audience, and all of the definitions being taken from the same source, but the ultimate accessibility being variable according to which KA was being drawn upon to provide the content.

This is not merely a case of people finding non-technical topics easier to interpret than technical ones, as we have the examples of the two distinct definitions/introductions to ‘passwords’ being drawn from two different KAs and landing very differently with the audiences. While the one drawn from WAM was generally considered to be digestible and in plain language, the one taken from AAA (which is arguably the KA in which readers would more naturally *expect* to find passwords being addressed, and so inclined to look at first) was complicated by the use of various elements of terminology (e.g. DIAMETER, HTTP Digest Authentication, RADIUS, salting, and shadow files). While all of these are potentially relevant to mention as someone seeks to go deeper into the topic, they are not applicable to a general ‘entry point’ on the topic (and indeed if the reader is already conversant with these terms, then they are unlikely to be needing to have passwords introduced to them in the first place).

The findings clearly indicate that, as currently presented, CyBOK is not ideally positioned for use by those from the non-cyber sectors. Even where they are sufficiently conversant with cyber security terminology to identify a topic to look for, the degree to which CyBOK then makes this accessible to them is mixed. While they may be able to *find* entries that appear to be of relevance in the Mapping

Reference, it is often far from clear which would be the primary place to look in terms of various KAs that may be highlighted. Moreover, even when the most relevant entry is determined, what the reader may find as a result is typically not framed in a manner that they would find understandable.

4.2 Reflections on responses from Cyber Sector participants

Having already had the experience of conducting the Law and Education sector workshops, the investigators had already had the experience of seeing how the non-expert participants had responded to CyBOK extracts for a variety of these KWoPs (with Data Protection, Passwords and Ransomware being used in the Law session, and Phishing and Ransomware featuring in the Education session). The Cyber sector respondents were of course able to offer a different perspective on the material, and notably made various comments about the accuracy and currency of the some of the statements being made. There was no doubt that they *understood* the descriptions, and there was instead a fairly significant degree of discussion about whether they *agreed* with them.

As highlighted in the earlier summary, various definitions (e.g. phishing, ransomware, and firewalls) were all considered to be outdated, and in some cases limited in scope. Some technical details being presented were considered to be rather niche (and could be worth cutting on this basis). The material was felt to be targeting an academic audience rather than an applied context. It was acknowledged that it is potentially not *possible* to dual-purpose the document – i.e. to practitioners and non-practitioners who will be looking for different things.

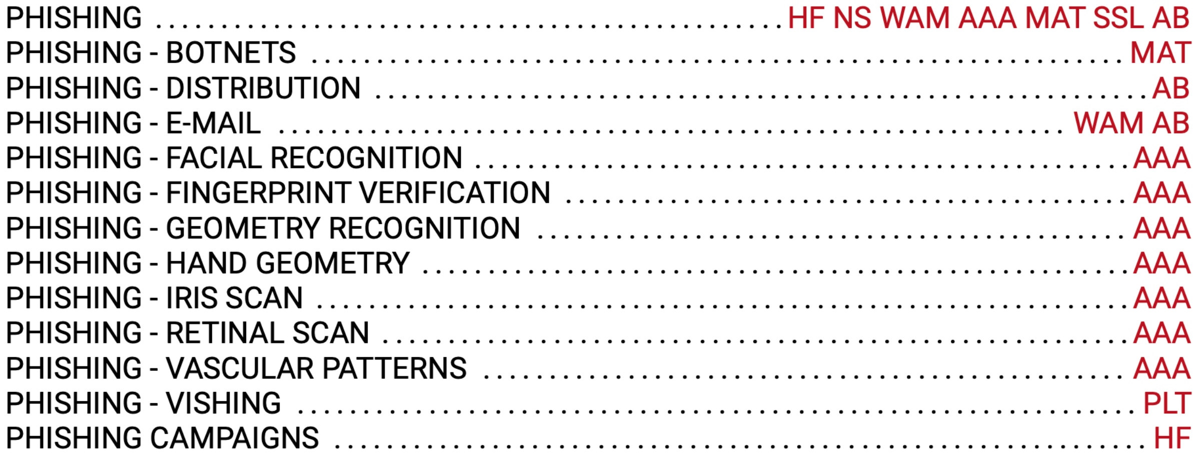
This potentially reflects a wider challenge for the maintenance of CyBOK, insofar as things *will* change and even if specific examples feel relevant and current *now*, they are liable to look and feel dated as time goes on.

4.3 Reflections on using the CyBOK Mapping Reference

There are issues in the way that the Mapping Reference presents its entries and what ‘mapping’ to the Knowledge Area is interpreted to mean as a consequence. As an example, Figure 5 presents the example of ‘Phishing’, which was identified as a KWoP by 12 of the survey respondents. The Figure shows that the KWoP on its own is mapped to seven distinct KAs, plus variations of the term have 12 further mapping entries[1]. Exploring these more fully in order to then try to identify a suitable definition/introduction/explanation for presentation to participants in related workshops, it then became clear that there was no obvious 'primary’ KA being highlighted. Looking across the seven that were listed, it transpired in this case that the last entry listed (Adversarial Behaviours) proved to be the best source for related text, with a fairly substantive portion of text being identified that served to outline what phishing is and how it is used (content from the Web & Mobile Security KA would have offered another reasonable option in this respect). Meanwhile, in several of the other KAs to which the KWoP was ‘mapped’, the associated mention of phishing was very much ‘in passing’

[1] It should be noted that ‘phishing’ is relatively modest in these respects compared to some other KWoPs, with ‘Password’ linking to eleven KAs and having 30+ further entries

rather than it being a focus topic (see, for example, the mentions offered in the AAA, MAT, NS and SSL Knowledge Areas). Looking at the wider list of mapping entries becomes rather curious insofar as there are 7 additional entries mapping to the AAA KA, linking phishing to a variety of biometrics. As it turns out, when looking for each of these biometrics in the KA text, none appear to be mentioned in the context of phishing (and indeed several of the biometrics – geometry recognition, hand geometry, retinal scan – are not mentioned at all). Similarly, while being listed in the mapping reference, the Physical Layer & Telecommunications Security KA makes no mention of phishing or vishing. This has clear potential to cause issues and misinterpretation if topics are then considered to link to particular KAs during activities such as qualification/certification mapping exercises without mappers actually checking the veracity of the mapping.



PHISHING	HF NS WAM AAA MAT SSL AB
PHISHING - BOTNETS	MAT
PHISHING - DISTRIBUTION	AB
PHISHING - E-MAIL	WAM AB
PHISHING - FACIAL RECOGNITION	AAA
PHISHING - FINGERPRINT VERIFICATION	AAA
PHISHING - GEOMETRY RECOGNITION	AAA
PHISHING - HAND GEOMETRY	AAA
PHISHING - IRIS SCAN	AAA
PHISHING - RETINAL SCAN	AAA
PHISHING - VASCULAR PATTERNS	AAA
PHISHING - VISHING	PLT
PHISHING CAMPAIGNS	HF

Figure 5 : Extract from the CyBOK Mapping Reference related to Phishing

The fact that tangible information about phishing could be found in at least the AB, WAM and (to a lesser extent) HF Knowledge Areas highlights a broader reflection on the use and utility of CyBOK, given the way in which the coverage of certain key topics is located in multiple places. In this particular case, if someone wants to get a clear sense of the Body of Knowledge that exists in relation to phishing, then the related text must be sought across several distinct KAs and it the reader does not get an integrated treatment of the topic. This proves to be far from an isolated example, and raises questions about the ways in which CyBOK (as currently structured) can be used most effectively. It could be relevant to consider some guidance on this aspect, so that would-be CyBOK users are supported to understand how best to approach different tasks according to their needs. For example, someone seeking to map a qualification to CyBOK is likely to use it in a rather different way to someone who is trying to learn more about a given topic (or topic area) and identify references to the wider body of knowledge that may exist about it.

5 Conclusions

The project as a whole, and the workshops in particular, provided insights with regard to making CyBOK more accessible or usable for wider audiences.

It was made apparent that the text is globally not accessible to non-practitioners, although there were exceptions. This highlights the heterogeneity of the reading level or technical level of the text and indicates that it is possible to make the text accessible, at least partially, and at least for some KWoPs.

The idea was evoked in the various workshops of splitting the technical and non-technical presentations in distinct parts, which would improve accessibility to non-experts. It was however commented during the Cyber sector workshop that it would be difficult to dual-purpose such a document.

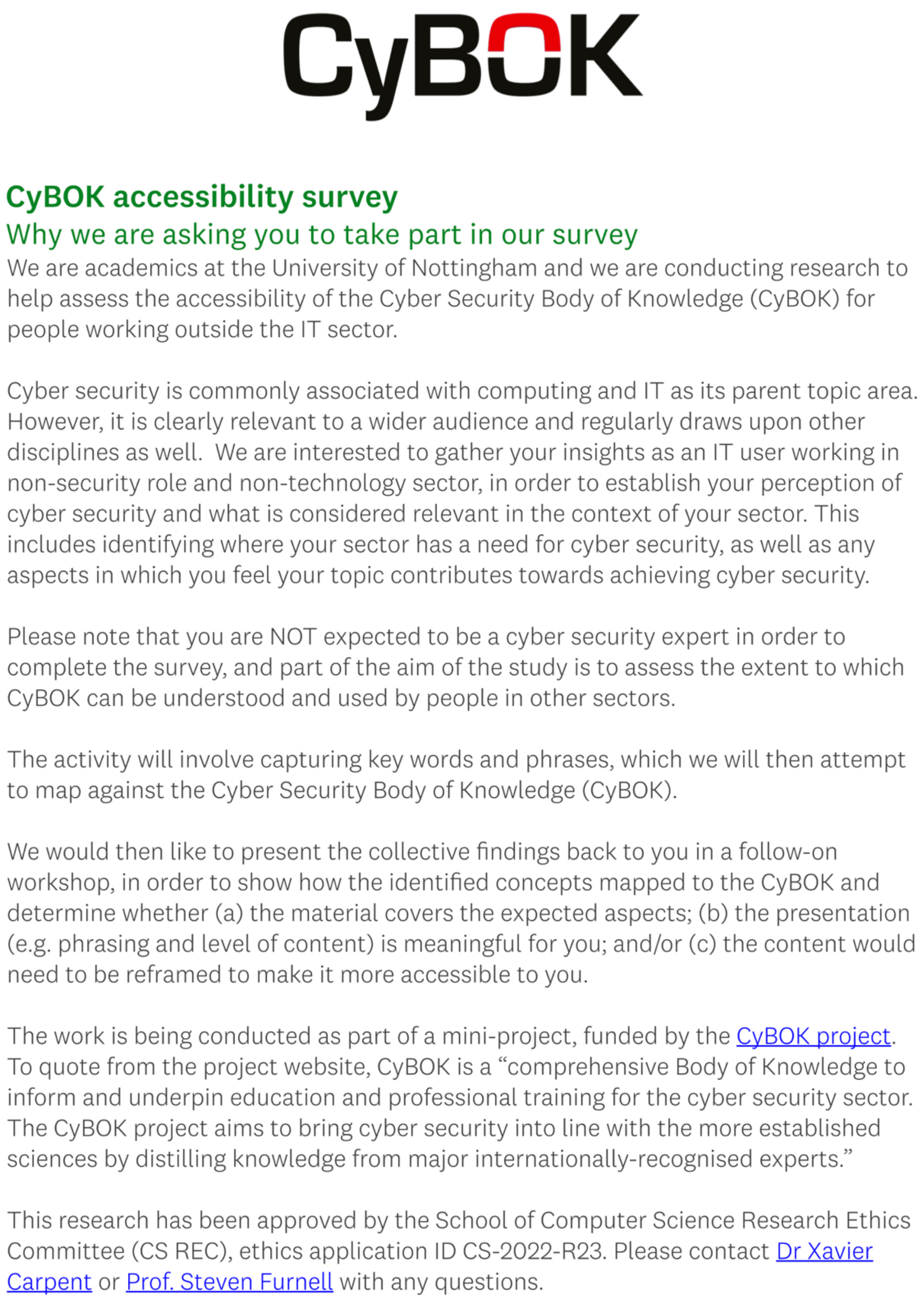
Another recurring theme was that of the practical accessibility and maintainability of CyBOK in its current form, namely a large document (possibly split in chapters/KAs) accompanied by a Mapping Reference. Participants often alluded to Wikipedia or a Wikipedia-like platform as a more appropriate format, with cross-referencing.

Finally, practitioners and non-practitioners alike expressed concerns regarding the rapidly evolving nature of the discipline, and questioned the ability of the current format to remain up-to-date. As a result, and in agreement with the previous observation, it may be worth exploring more flexible formats for future iterations of CyBOK.

Overall, it can be concluded that, on one level, the findings support the desirability of further exploring the idea of a 'sector lens' approach for CyBOK. There is clear recognition of the relevance of both the broad issue and the individual KA topics from the perspective of all of the wider (non-cyber) sector respondents and participants. At the same time, the actual realisation of this would appear to be challenging from the basis of the current content and structure of the CyBOK material. Accessibility to other sectors would potentially be eased by a more granular and layered approach to the content, which could then enable key topics to be segmented into layperson and technical/practitioner versions of material, and with references to the wider body of knowledge also differentiated based on the audiences that would find the resulting material most accessible. If taken forward, this would clearly represent a considerable further development of the CyBOK work, but at the same time would serve to increase its accessibility (and potential utility) for a wider audience.

Appendix A: CyBOK Accessibility Survey

The following pages present a copy of the questionnaire instrument (including briefing details), as presented to respondents on the SurveyMonkey site.



CyBOK accessibility survey

Why we are asking you to take part in our survey

We are academics at the University of Nottingham and we are conducting research to help assess the accessibility of the Cyber Security Body of Knowledge (CyBOK) for people working outside the IT sector.

Cyber security is commonly associated with computing and IT as its parent topic area. However, it is clearly relevant to a wider audience and regularly draws upon other disciplines as well. We are interested to gather your insights as an IT user working in non-security role and non-technology sector, in order to establish your perception of cyber security and what is considered relevant in the context of your sector. This includes identifying where your sector has a need for cyber security, as well as any aspects in which you feel your topic contributes towards achieving cyber security.

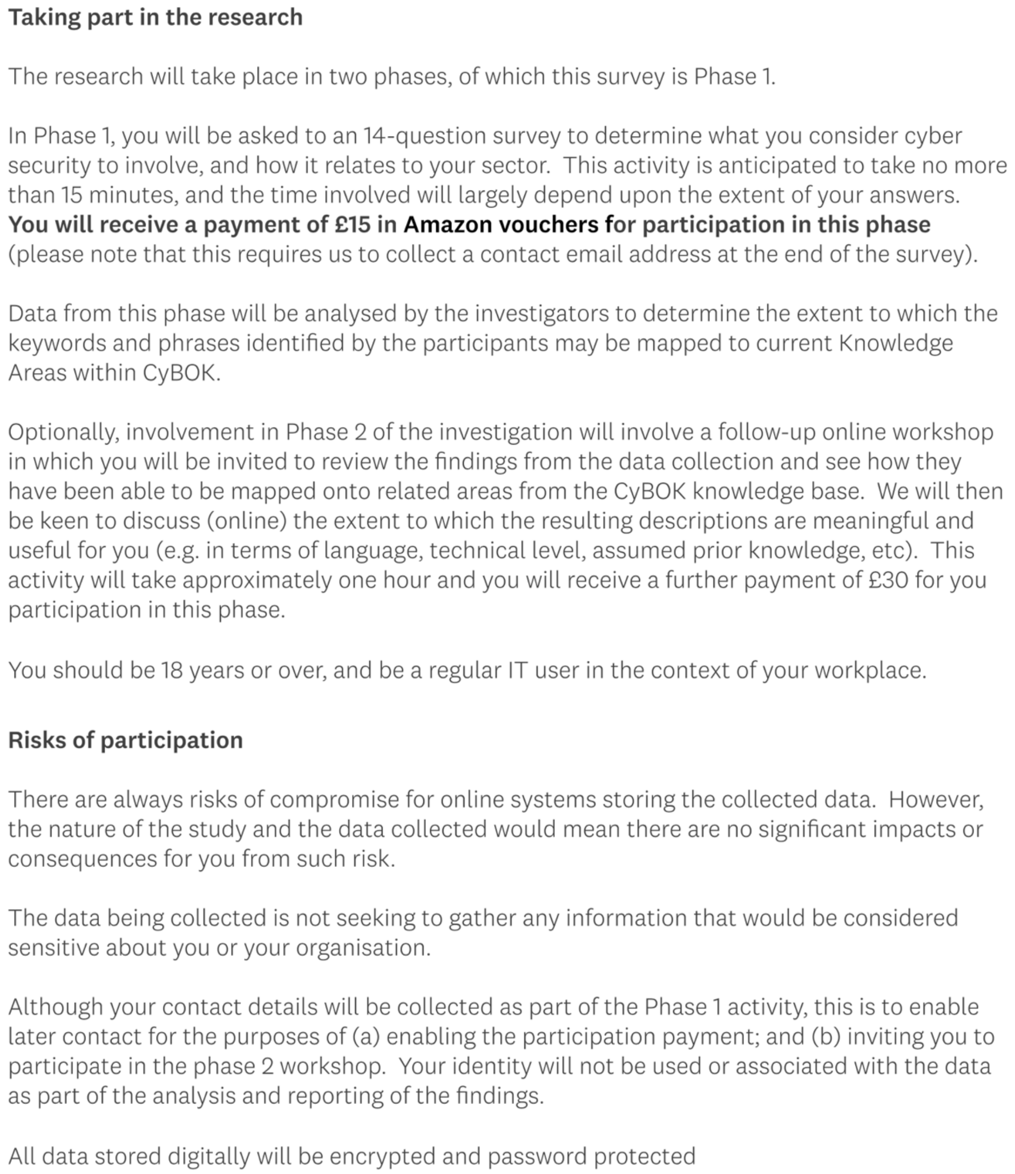
Please note that you are NOT expected to be a cyber security expert in order to complete the survey, and part of the aim of the study is to assess the extent to which CyBOK can be understood and used by people in other sectors.

The activity will involve capturing key words and phrases, which we will then attempt to map against the Cyber Security Body of Knowledge (CyBOK).

We would then like to present the collective findings back to you in a follow-on workshop, in order to show how the identified concepts mapped to the CyBOK and determine whether (a) the material covers the expected aspects; (b) the presentation (e.g. phrasing and level of content) is meaningful for you; and/or (c) the content would need to be reframed to make it more accessible to you.

The work is being conducted as part of a mini-project, funded by the CyBOK project. To quote from the project website, CyBOK is a "comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector. The CyBOK project aims to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts."

This research has been approved by the School of Computer Science Research Ethics Committee (CS REC), ethics application ID CS-2022-R23. Please contact Dr Xavier Carpent or Prof. Steven Furnell with any questions.



Taking part in the research

The research will take place in two phases, of which this survey is Phase 1.

In Phase 1, you will be asked to an 14-question survey to determine what you consider cyber security to involve, and how it relates to your sector. This activity is anticipated to take no more than 15 minutes, and the time involved will largely depend upon the extent of your answers. **You will receive a payment of £15 in Amazon vouchers for participation in this phase** (please note that this requires us to collect a contact email address at the end of the survey).

Data from this phase will be analysed by the investigators to determine the extent to which the keywords and phrases identified by the participants may be mapped to current Knowledge Areas within CyBOK.

Optionally, involvement in Phase 2 of the investigation will involve a follow-up online workshop in which you will be invited to review the findings from the data collection and see how they have been able to be mapped onto related areas from the CyBOK knowledge base. We will then be keen to discuss (online) the extent to which the resulting descriptions are meaningful and useful for you (e.g. in terms of language, technical level, assumed prior knowledge, etc). This activity will take approximately one hour and you will receive a further payment of £30 for you participation in this phase.

You should be 18 years or over, and be a regular IT user in the context of your workplace.

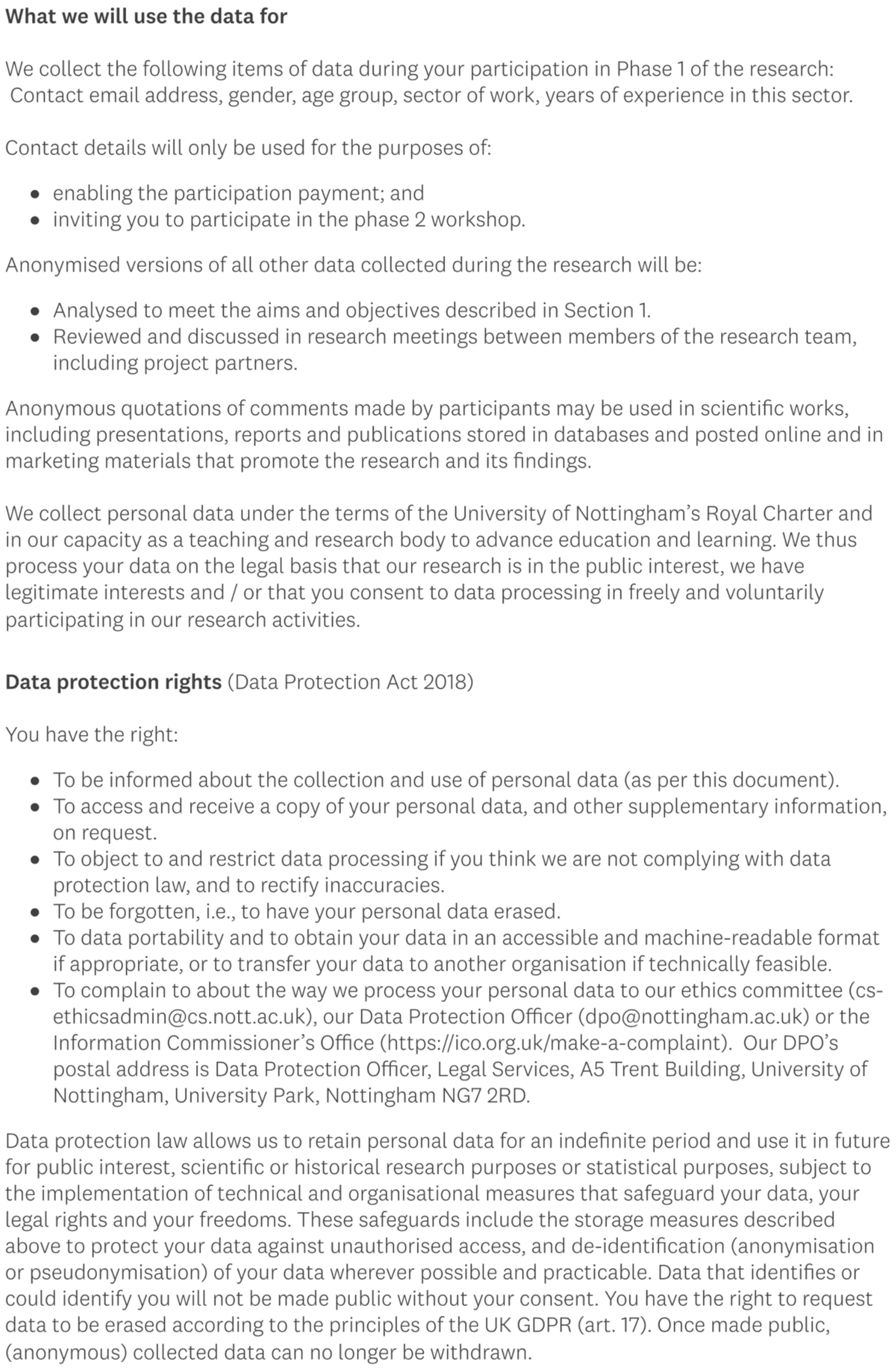
Risks of participation

There are always risks of compromise for online systems storing the collected data. However, the nature of the study and the data collected would mean there are no significant impacts or consequences for you from such risk.

The data being collected is not seeking to gather any information that would be considered sensitive about you or your organisation.

Although your contact details will be collected as part of the Phase 1 activity, this is to enable later contact for the purposes of (a) enabling the participation payment; and (b) inviting you to participate in the phase 2 workshop. Your identity will not be used or associated with the data as part of the analysis and reporting of the findings.

All data stored digitally will be encrypted and password protected



What we will use the data for

We collect the following items of data during your participation in Phase 1 of the research: Contact email address, gender, age group, sector of work, years of experience in this sector.

Contact details will only be used for the purposes of:

- enabling the participation payment; and
- inviting you to participate in the phase 2 workshop.

Anonymised versions of all other data collected during the research will be:

- Analysed to meet the aims and objectives described in Section 1.
- Reviewed and discussed in research meetings between members of the research team, including project partners.

Anonymous quotations of comments made by participants may be used in scientific works, including presentations, reports and publications stored in databases and posted online and in marketing materials that promote the research and its findings.

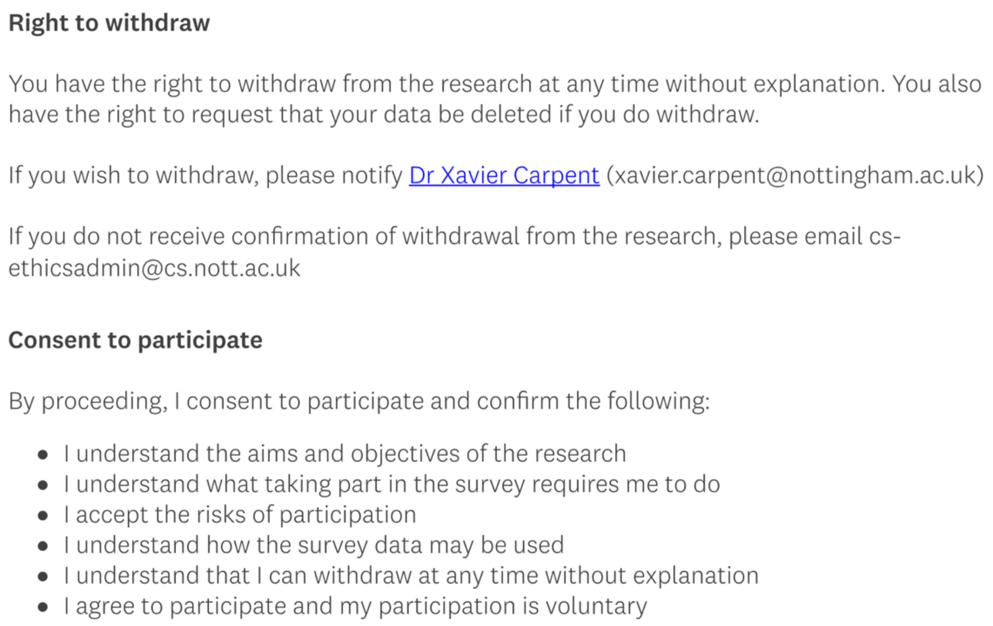
We collect personal data under the terms of the University of Nottingham's Royal Charter and in our capacity as a teaching and research body to advance education and learning. We thus process your data on the legal basis that our research is in the public interest, we have legitimate interests and / or that you consent to data processing in freely and voluntarily participating in our research activities.

Data protection rights (Data Protection Act 2018)

You have the right:

- To be informed about the collection and use of personal data (as per this document).
- To access and receive a copy of your personal data, and other supplementary information, on request.
- To object to and restrict data processing if you think we are not complying with data protection law, and to rectify inaccuracies.
- To be forgotten, i.e., to have your personal data erased.
- To data portability and to obtain your data in an accessible and machine-readable format if appropriate, or to transfer your data to another organisation if technically feasible.
- To complain to about the way we process your personal data to our ethics committee (cs-ethicsadmin@cs.nott.ac.uk), our Data Protection Officer (dpo@nottingham.ac.uk) or the Information Commissioner's Office (https://ico.org.uk/make-a-complaint). Our DPO's postal address is Data Protection Officer, Legal Services, A5 Trent Building, University of Nottingham, University Park, Nottingham NG7 2RD.

Data protection law allows us to retain personal data for an indefinite period and use it in future for public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of technical and organisational measures that safeguard your data, your legal rights and your freedoms. These safeguards include the storage measures described above to protect your data against unauthorised access, and de-identification (anonymisation or pseudonymisation) of your data wherever possible and practicable. Data that identifies or could identify you will not be made public without your consent. You have the right to request data to be erased according to the principles of the UK GDPR (art. 17). Once made public, (anonymous) collected data can no longer be withdrawn.



Right to withdraw

You have the right to withdraw from the research at any time without explanation. You also have the right to request that your data be deleted if you do withdraw.

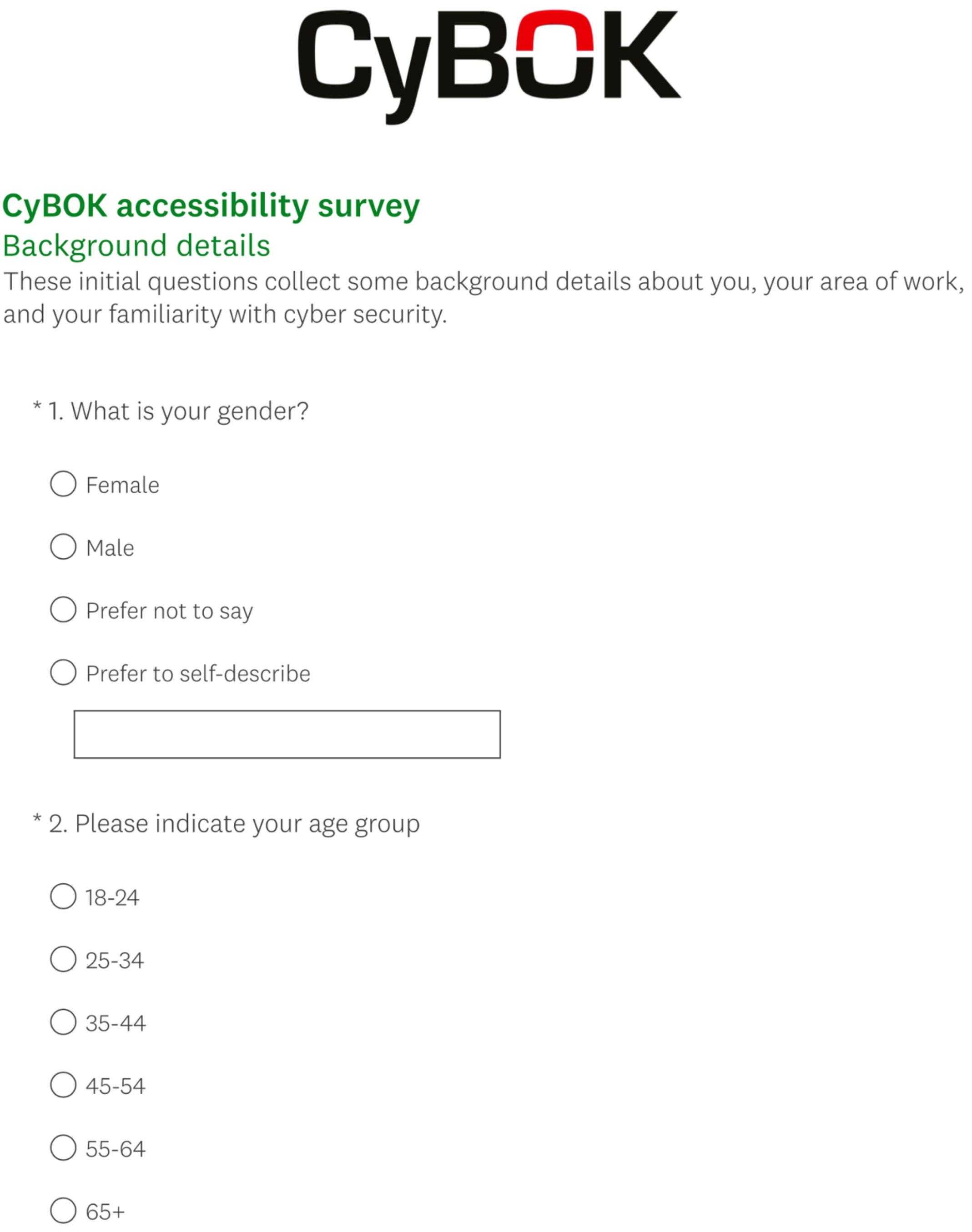
If you wish to withdraw, please notify Dr Xavier Carpent (xavier.carpent@nottingham.ac.uk)

If you do not receive confirmation of withdrawal from the research, please email cs-ethicsadmin@cs.nott.ac.uk

Consent to participate

By proceeding, I consent to participate and confirm the following:

- I understand the aims and objectives of the research
- I understand what taking part in the survey requires me to do
- I accept the risks of participation
- I understand how the survey data may be used
- I understand that I can withdraw at any time without explanation
- I agree to participate and my participation is voluntary



CyBOK

CyBOK accessibility survey

Background details

These initial questions collect some background details about you, your area of work, and your familiarity with cyber security.

* 1. What is your gender?

○ Female

○ Male

○ Prefer not to say

○ Prefer to self-describe

* 2. Please indicate your age group

○ 18-24

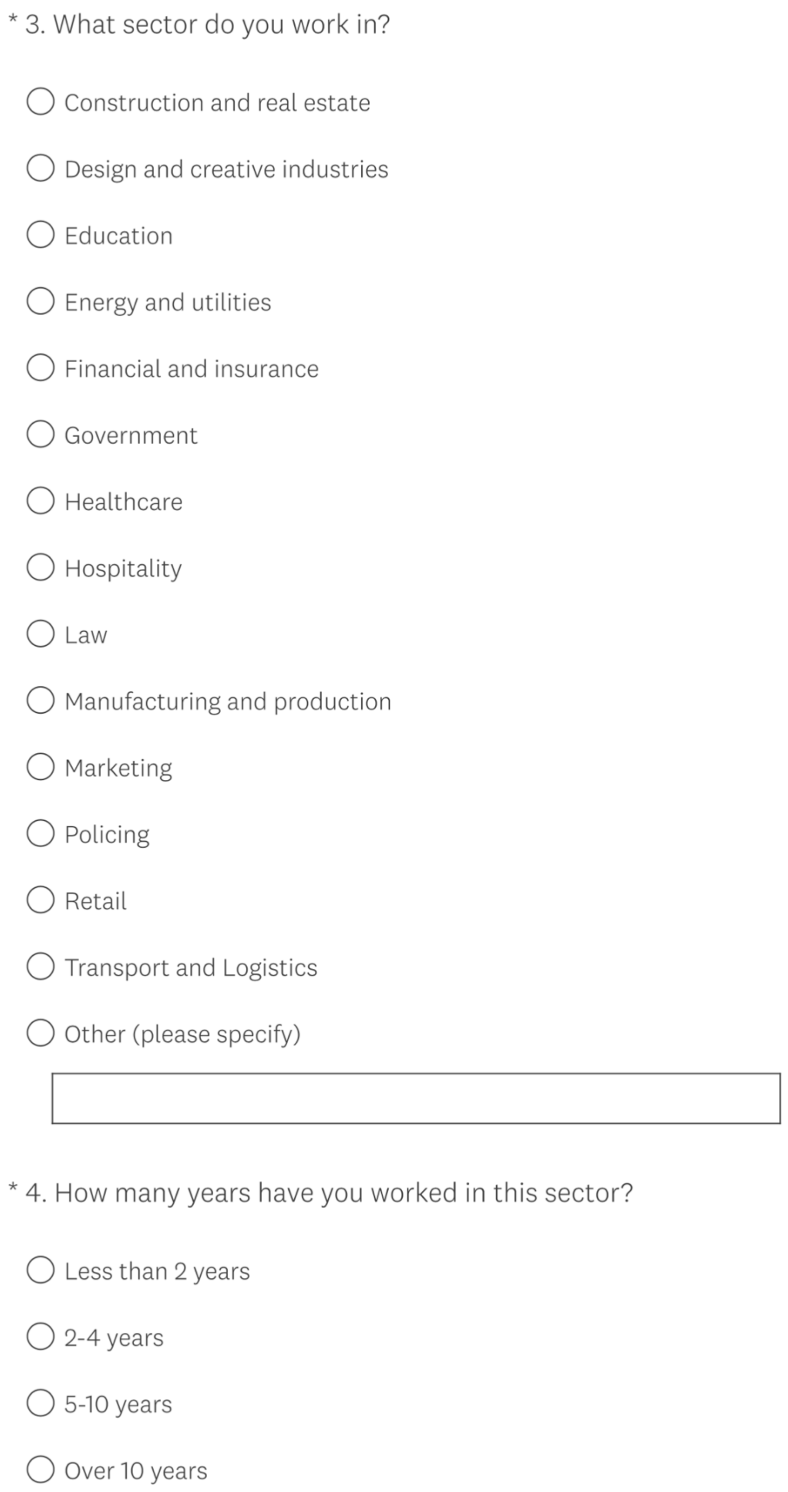
○ 25-34

○ 35-44

○ 45-54

○ 55-64

○ 65+



* 3. What sector do you work in?

○ Construction and real estate

○ Design and creative industries

○ Education

○ Energy and utilities

○ Financial and insurance

○ Government

○ Healthcare

○ Hospitality

○ Law

○ Manufacturing and production

○ Marketing

○ Policing

○ Retail

○ Transport and Logistics

○ Other (please specify)

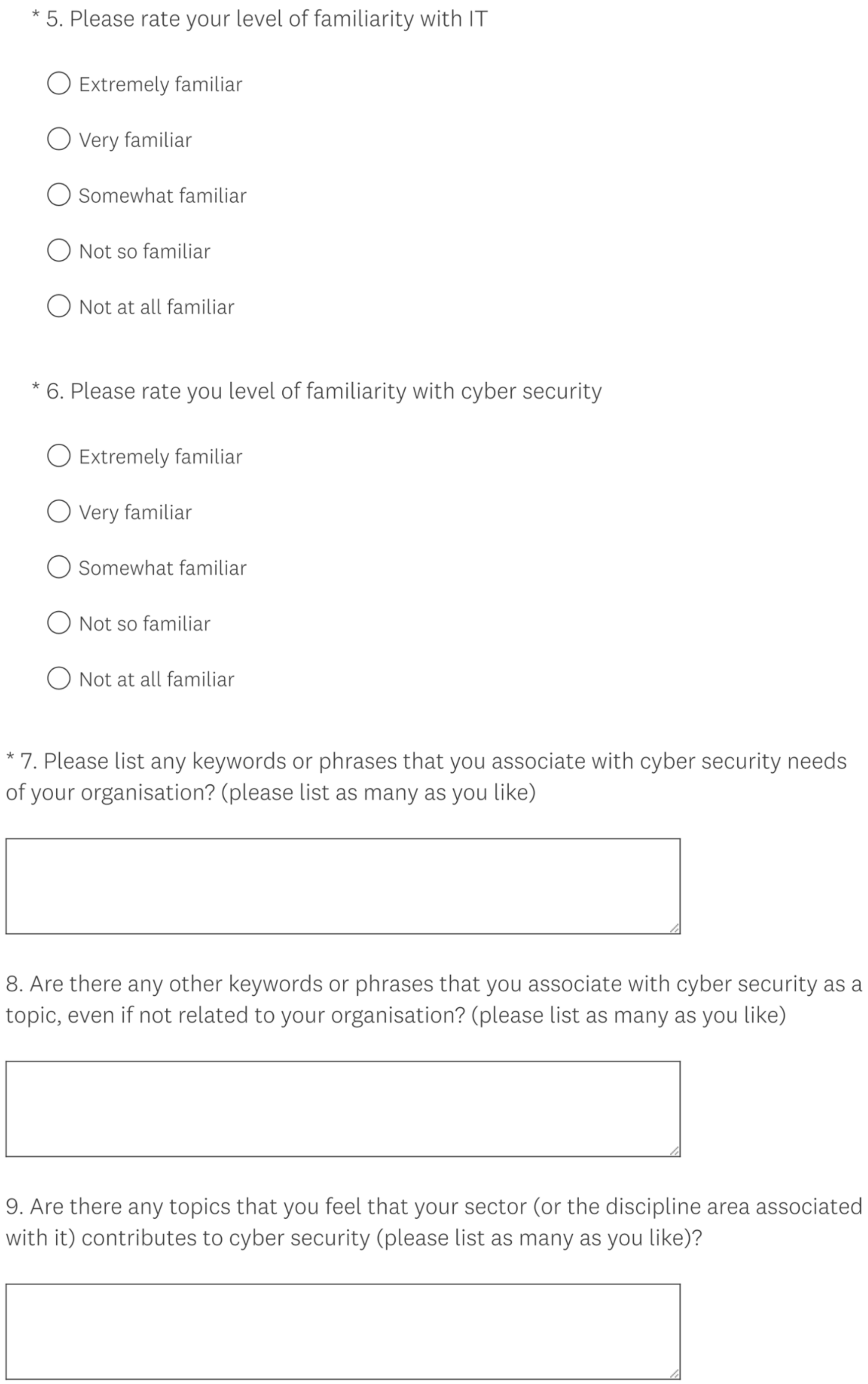
* 4. How many years have you worked in this sector?

○ Less than 2 years

○ 2-4 years

○ 5-10 years

○ Over 10 years



* 5. Please rate your level of familiarity with IT

○ Extremely familiar

○ Very familiar

○ Somewhat familiar

○ Not so familiar

○ Not at all familiar

* 6. Please rate you level of familiarity with cyber security

○ Extremely familiar

○ Very familiar

○ Somewhat familiar

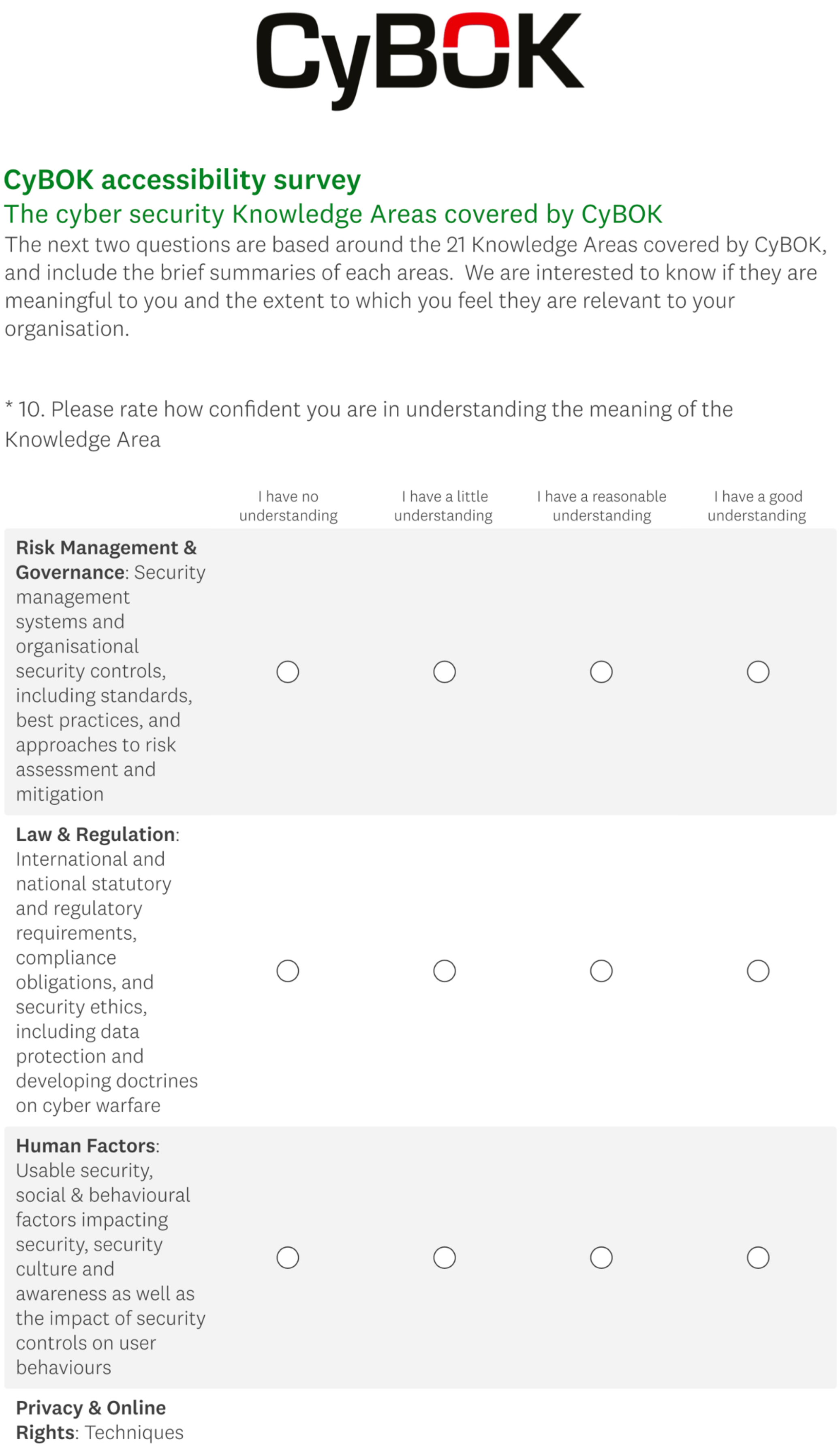
○ Not so familiar

○ Not at all familiar

* 7. Please list any keywords or phrases that you associate with cyber security needs of your organisation? (please list as many as you like)

8. Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation? (please list as many as you like)

9. Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security (please list as many as you like)?



CyBOK

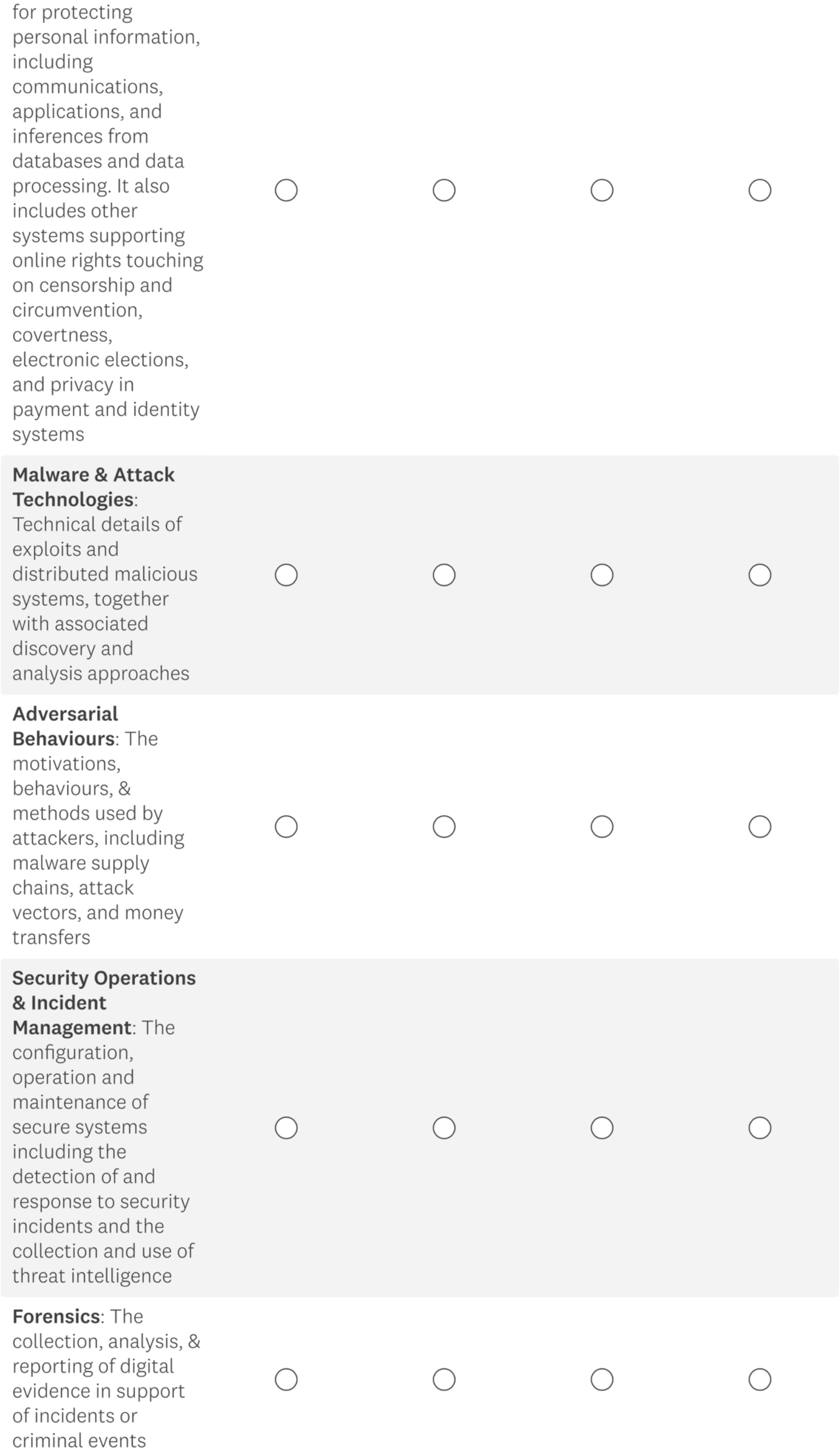
CyBOK accessibility survey

The cyber security Knowledge Areas covered by CyBOK

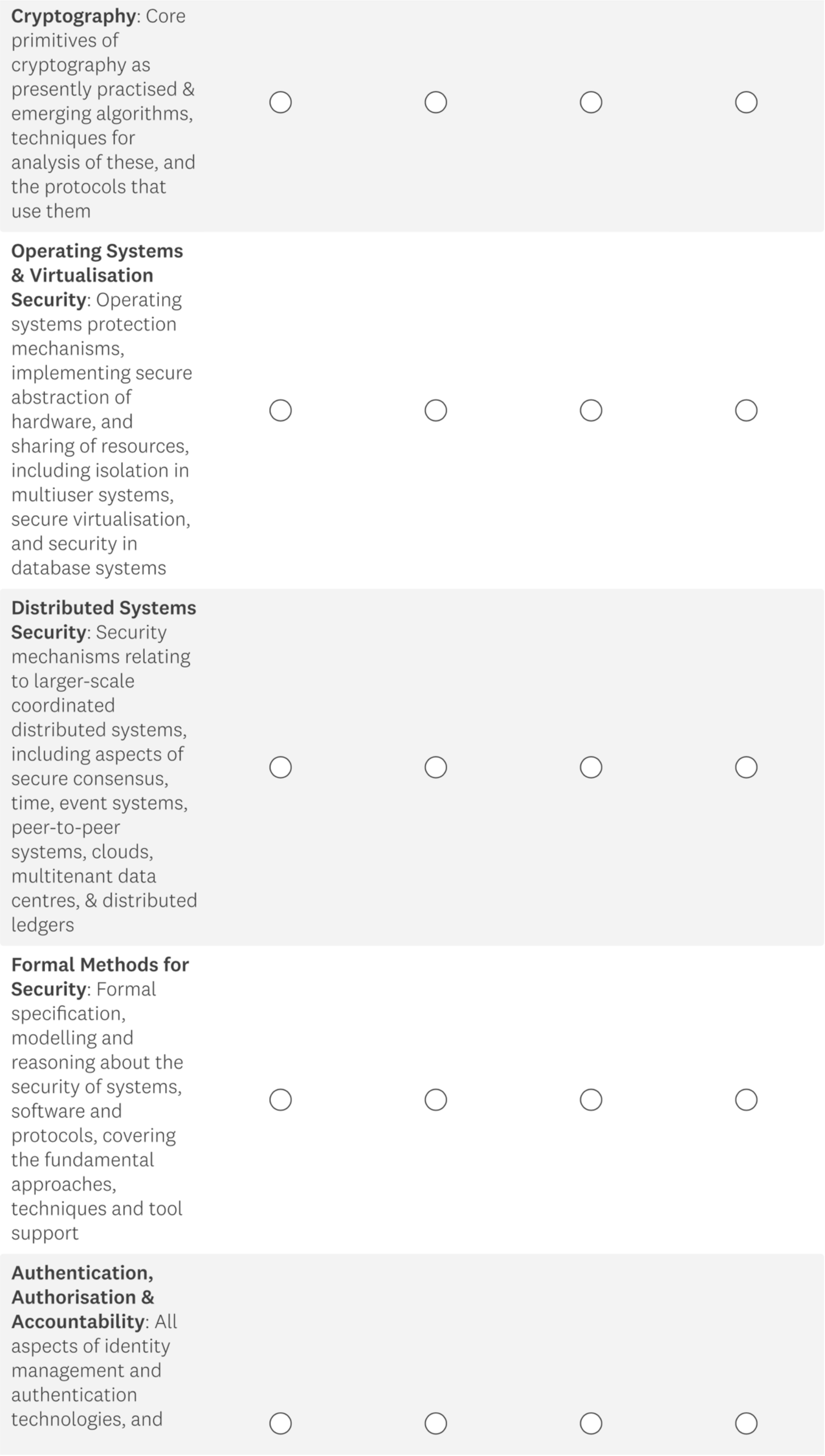
The next two questions are based around the 21 Knowledge Areas covered by CyBOK, and include the brief summaries of each areas. We are interested to know if they are meaningful to you and the extent to which you feel they are relevant to your organisation.

* 10. Please rate how confident you are in understanding the meaning of the Knowledge Area

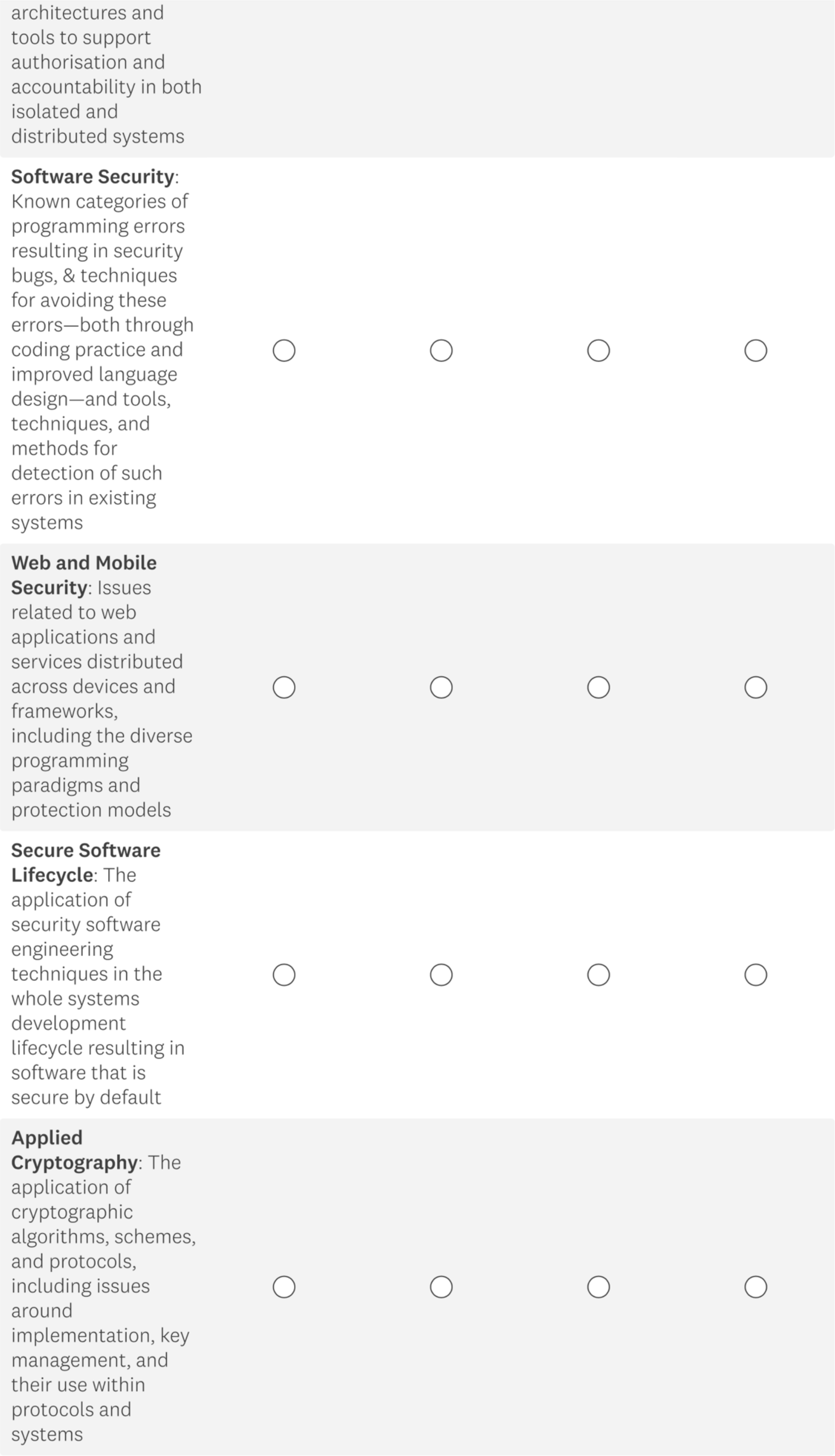
	I have no understanding	I have a little understanding	I have a reasonable understanding	I have a good understanding
Risk Management & Governance: Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation	○	○	○	○
Law & Regulation: International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare	○	○	○	○
Human Factors: Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours	○	○	○	○
Privacy & Online Rights: Techniques				



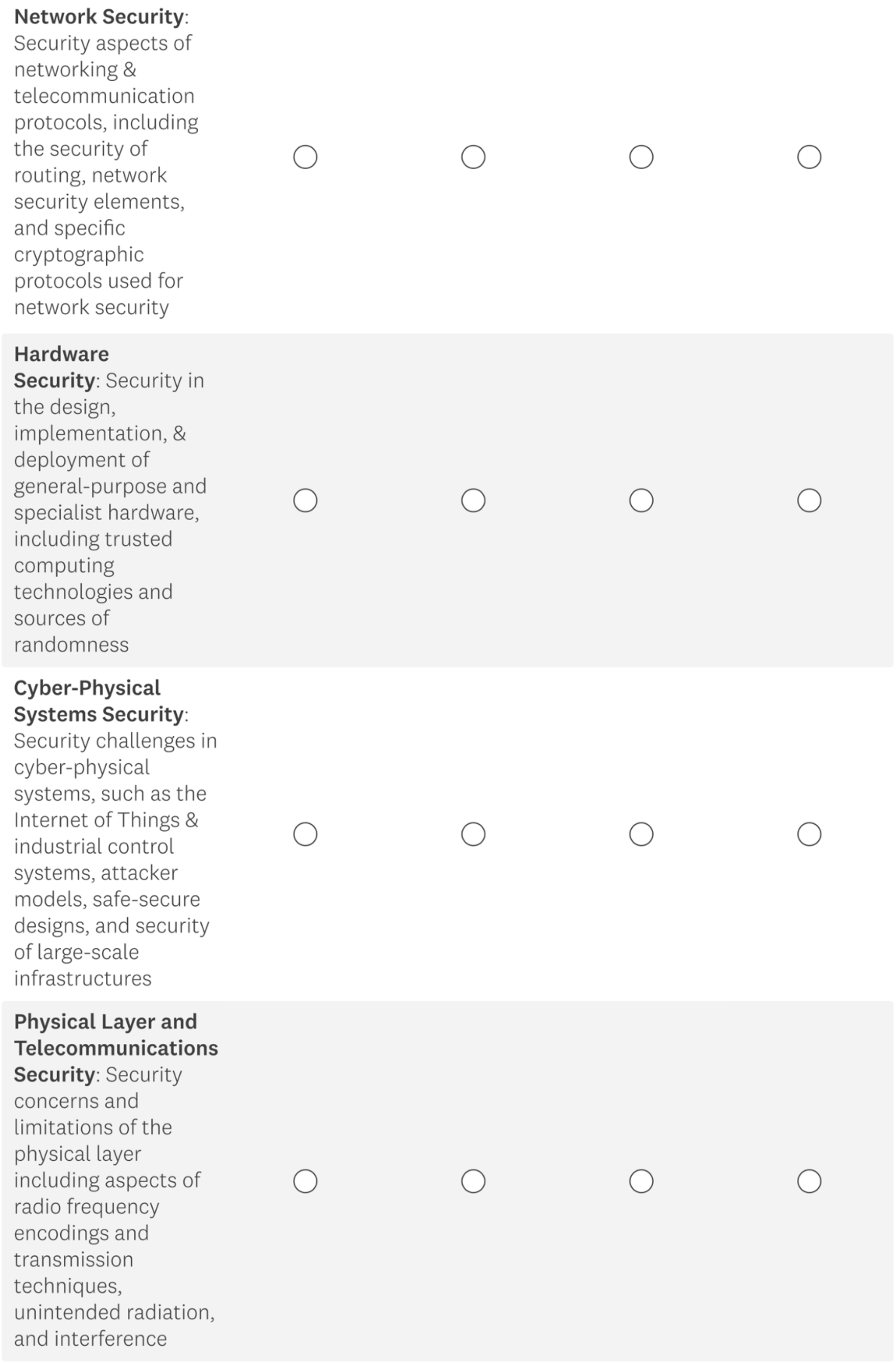
for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems	○	○	○	○
Malware & Attack Technologies: Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches	○	○	○	○
Adversarial Behaviours: The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers	○	○	○	○
Security Operations & Incident Management: The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence	○	○	○	○
Forensics: The collection, analysis, & reporting of digital evidence in support of incidents or criminal events	○	○	○	○



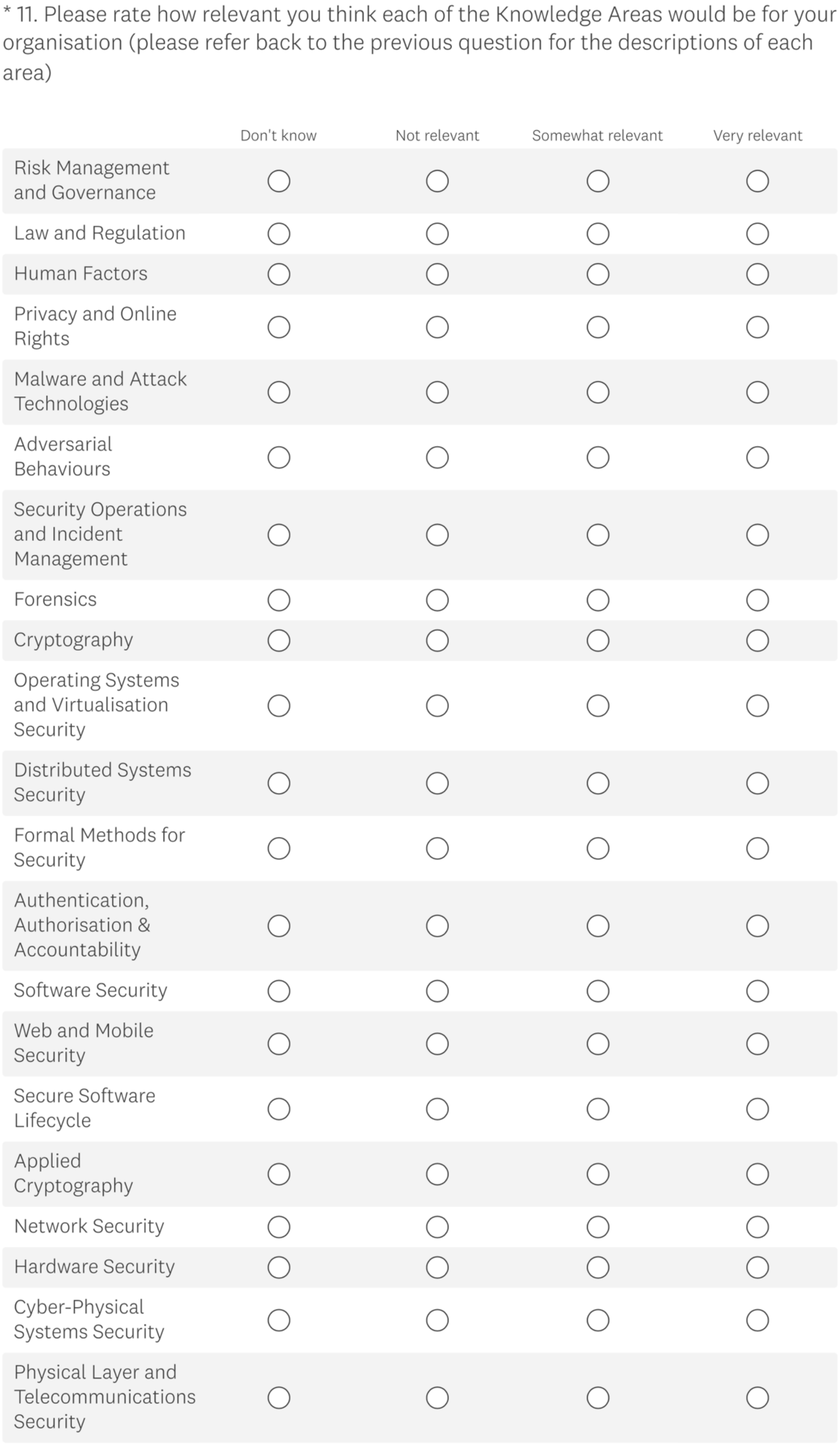
Cryptography: Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them	○	○	○	○
Operating Systems & Virtualisation Security: Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems	○	○	○	○
Distributed Systems Security: Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers	○	○	○	○
Formal Methods for Security: Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support	○	○	○	○
Authentication, Authorisation & Accountability: All aspects of identity management and authentication technologies, and	○	○	○	○



architectures and tools to support authorisation and accountability in both isolated and distributed systems				
Software Security: Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems	○	○	○	○
Web and Mobile Security: Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models	○	○	○	○
Secure Software Lifecycle: The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default	○	○	○	○
Applied Cryptography: The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems	○	○	○	○

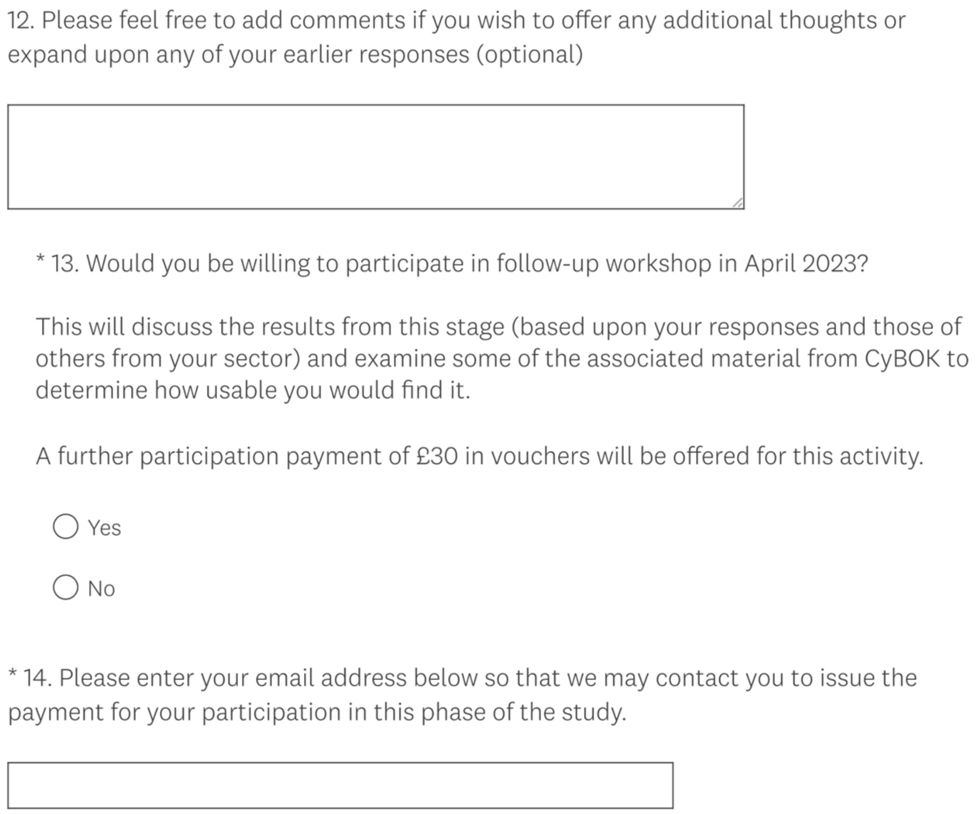


Network Security: Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security	○	○	○	○
Hardware Security: Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness	○	○	○	○
Cyber-Physical Systems Security: Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures	○	○	○	○
Physical Layer and Telecommunications Security: Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference	○	○	○	○



* 11. Please rate how relevant you think each of the Knowledge Areas would be for your organisation (please refer back to the previous question for the descriptions of each area)

	Don't know	Not relevant	Somewhat relevant	Very relevant
Risk Management and Governance	○	○	○	○
Law and Regulation	○	○	○	○
Human Factors	○	○	○	○
Privacy and Online Rights	○	○	○	○
Malware and Attack Technologies	○	○	○	○
Adversarial Behaviours	○	○	○	○
Security Operations and Incident Management	○	○	○	○
Forensics	○	○	○	○
Cryptography	○	○	○	○
Operating Systems and Virtualisation Security	○	○	○	○
Distributed Systems Security	○	○	○	○
Formal Methods for Security	○	○	○	○
Authentication, Authorisation & Accountability	○	○	○	○
Software Security	○	○	○	○
Web and Mobile Security	○	○	○	○
Secure Software Lifecycle	○	○	○	○
Applied Cryptography	○	○	○	○
Network Security	○	○	○	○
Hardware Security	○	○	○	○
Cyber-Physical Systems Security	○	○	○	○
Physical Layer and Telecommunications Security	○	○	○	○



12. Please feel free to add comments if you wish to offer any additional thoughts or expand upon any of your earlier responses (optional)

* 13. Would you be willing to participate in follow-up workshop in April 2023?

This will discuss the results from this stage (based upon your responses and those of others from your sector) and examine some of the associated material from CyBOK to determine how usable you would find it.

A further participation payment of £30 in vouchers will be offered for this activity.

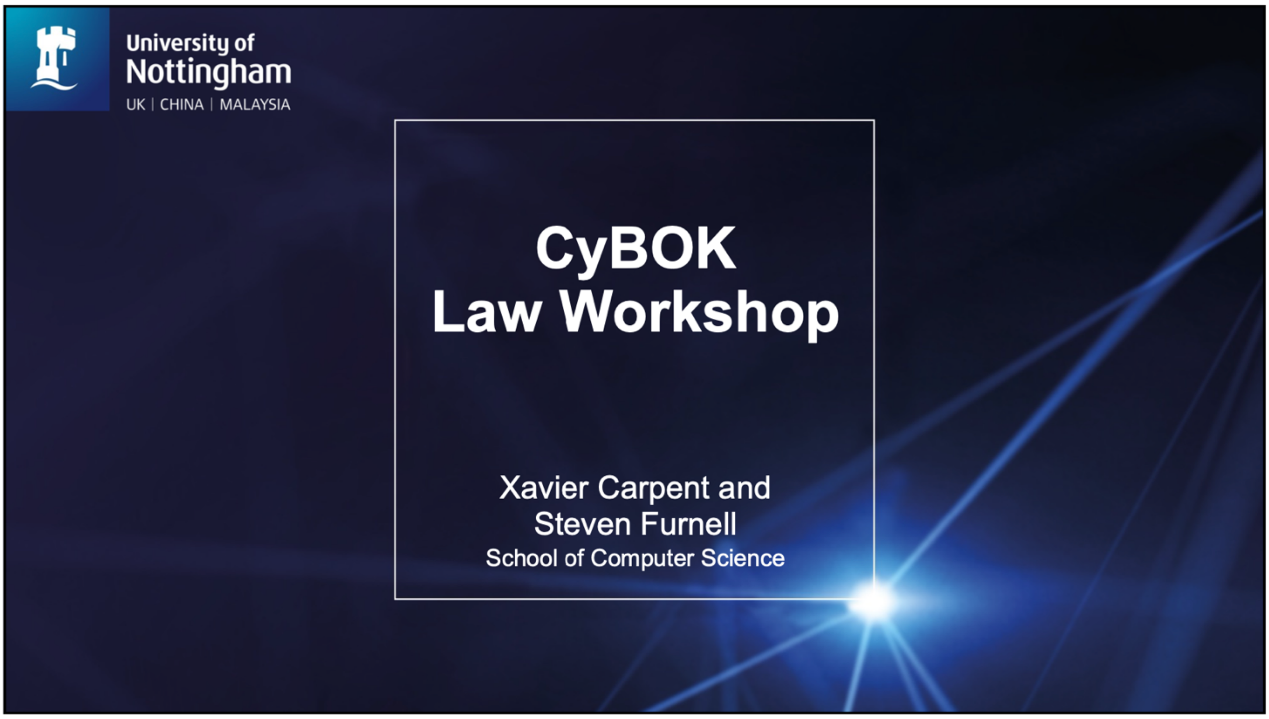
○ Yes

○ No

* 14. Please enter your email address below so that we may contact you to issue the payment for your participation in this phase of the study.

Appendix B: Example of Workshop session slides

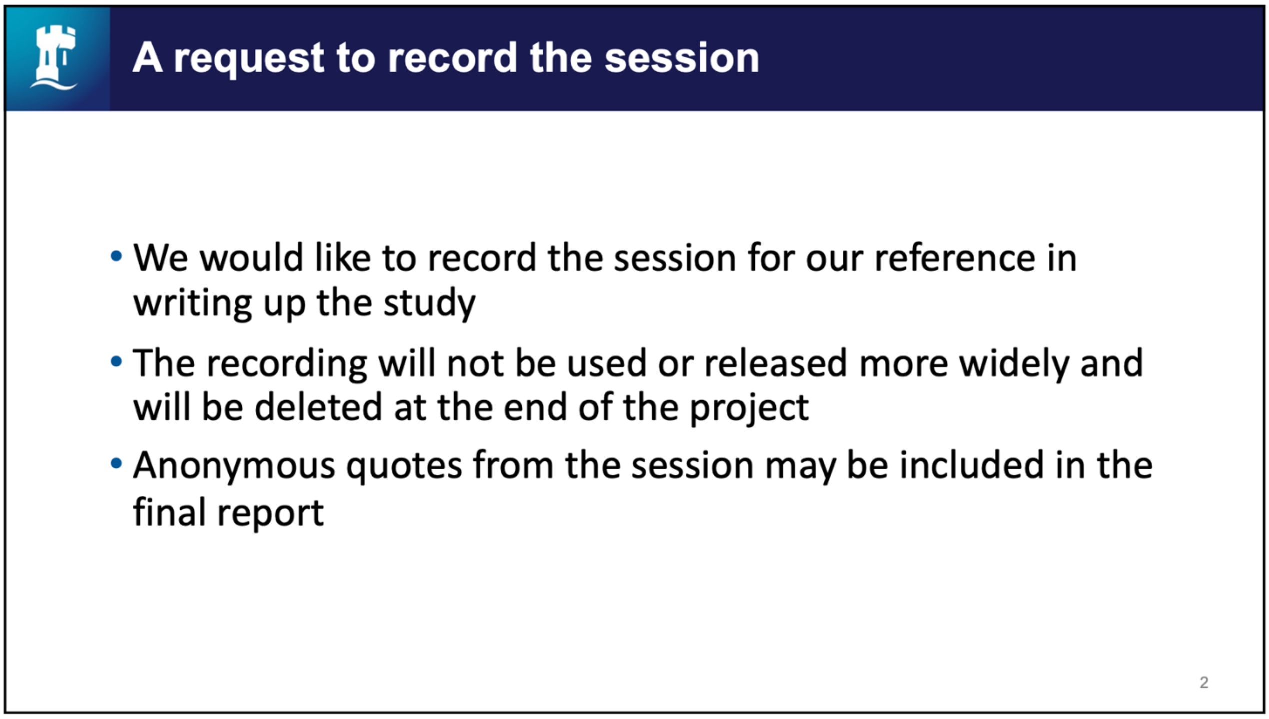
The following pages present an example of the slides used to support each of the workshop sessions. In this case, the example is taken from the Law sector session.



University of Nottingham
UK | CHINA | MALAYSIA

CyBOK Law Workshop

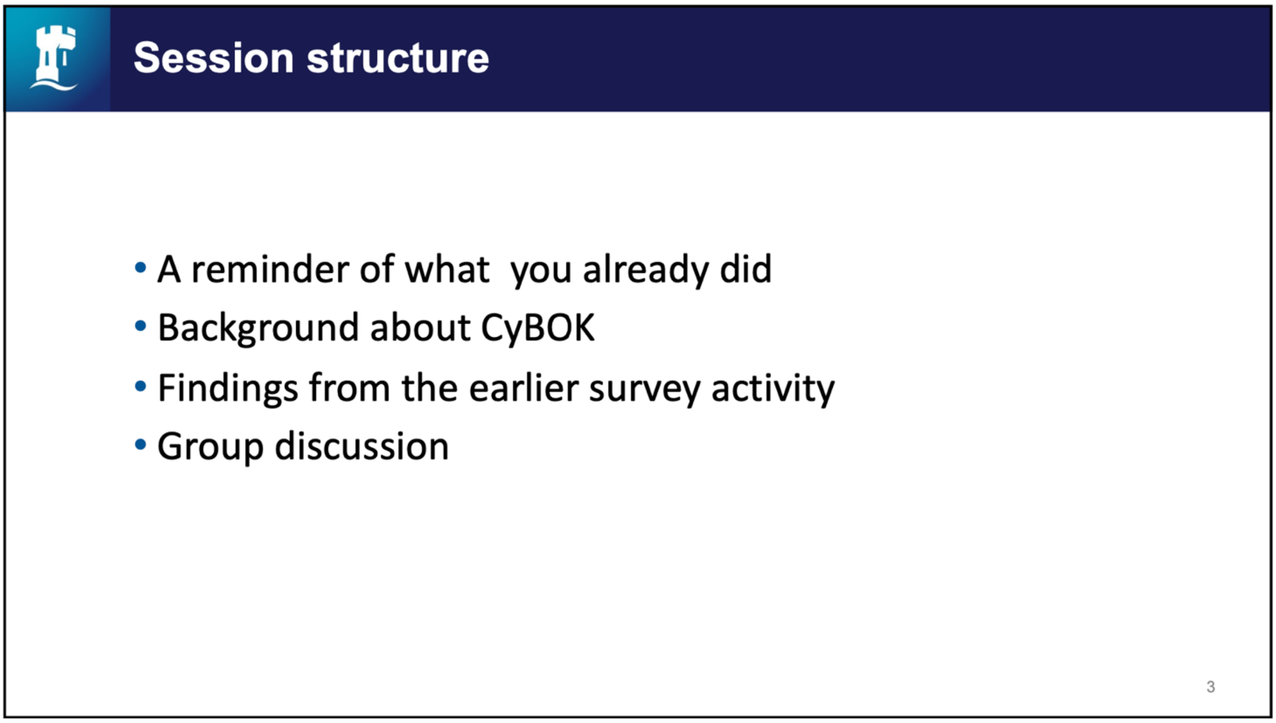
Xavier Carpent and
Steven Furnell
School of Computer Science



A request to record the session

- We would like to record the session for our reference in writing up the study
- The recording will not be used or released more widely and will be deleted at the end of the project
- Anonymous quotes from the session may be included in the final report

2



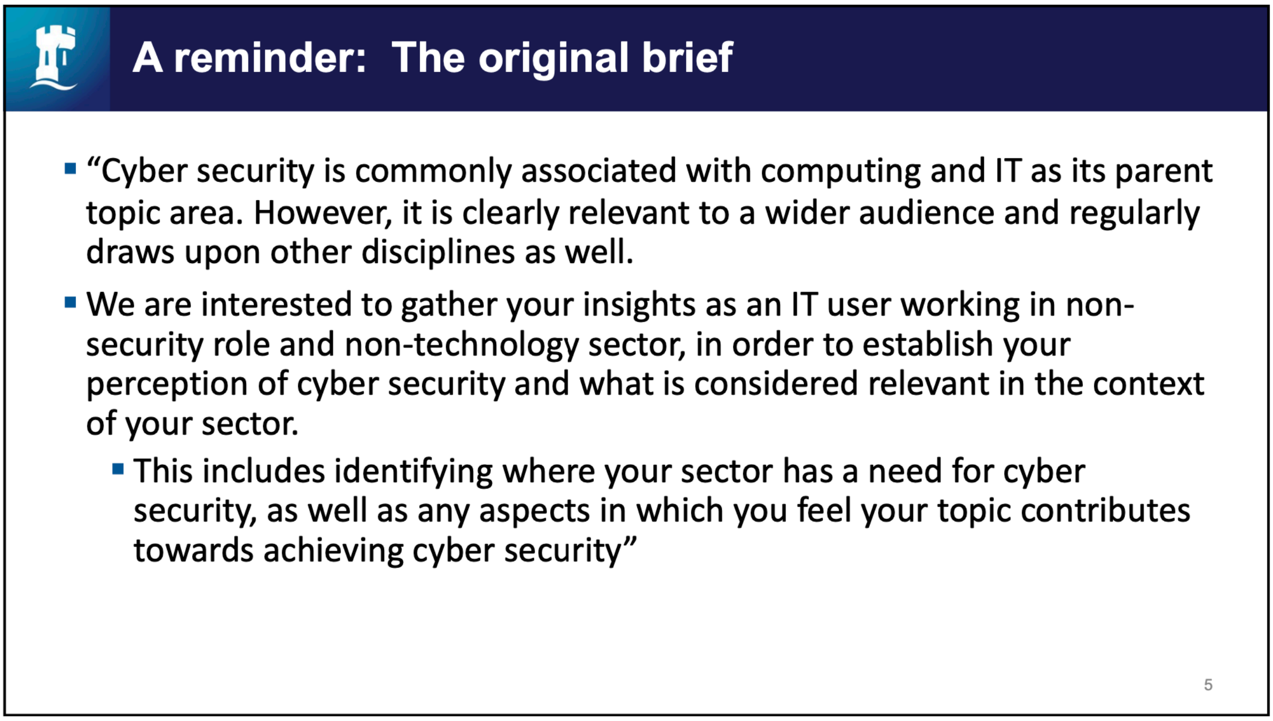
Session structure

- A reminder of what you already did
- Background about CyBOK
- Findings from the earlier survey activity
- Group discussion

3

Background

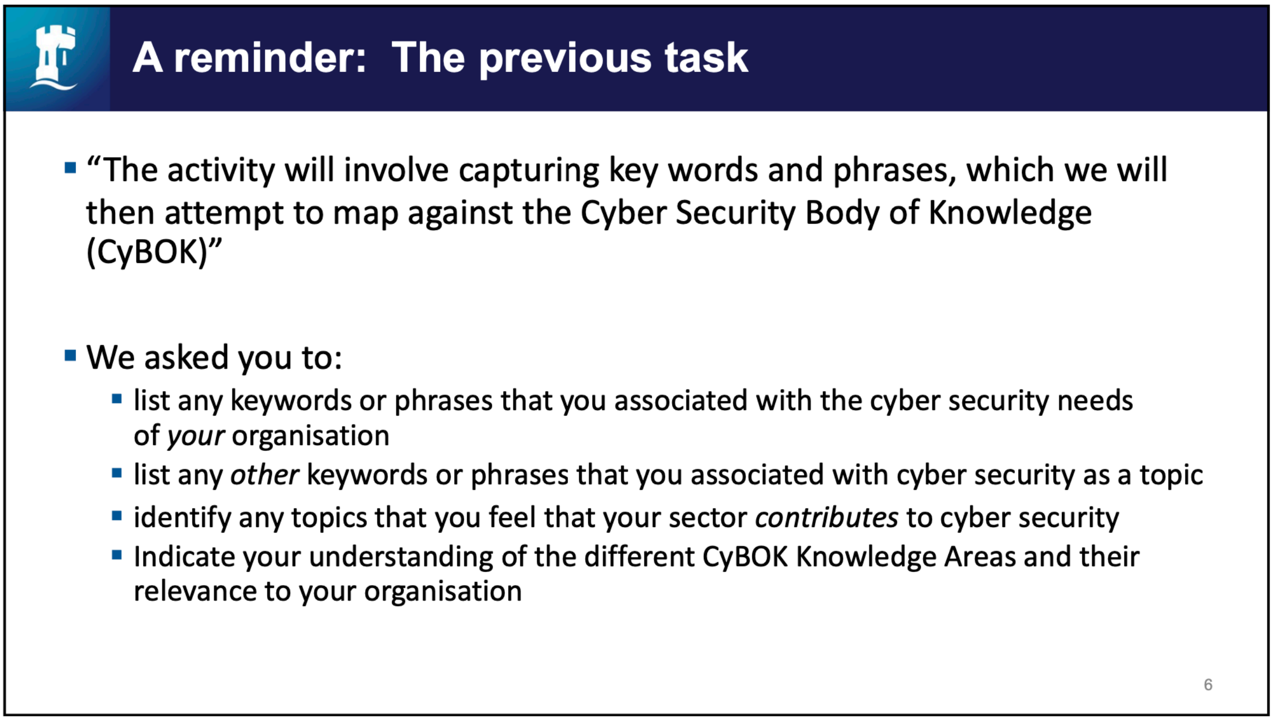
4



A reminder: The original brief

- “Cyber security is commonly associated with computing and IT as its parent topic area. However, it is clearly relevant to a wider audience and regularly draws upon other disciplines as well.
- We are interested to gather your insights as an IT user working in non-security role and non-technology sector, in order to establish your perception of cyber security and what is considered relevant in the context of your sector.
  - This includes identifying where your sector has a need for cyber security, as well as any aspects in which you feel your topic contributes towards achieving cyber security”

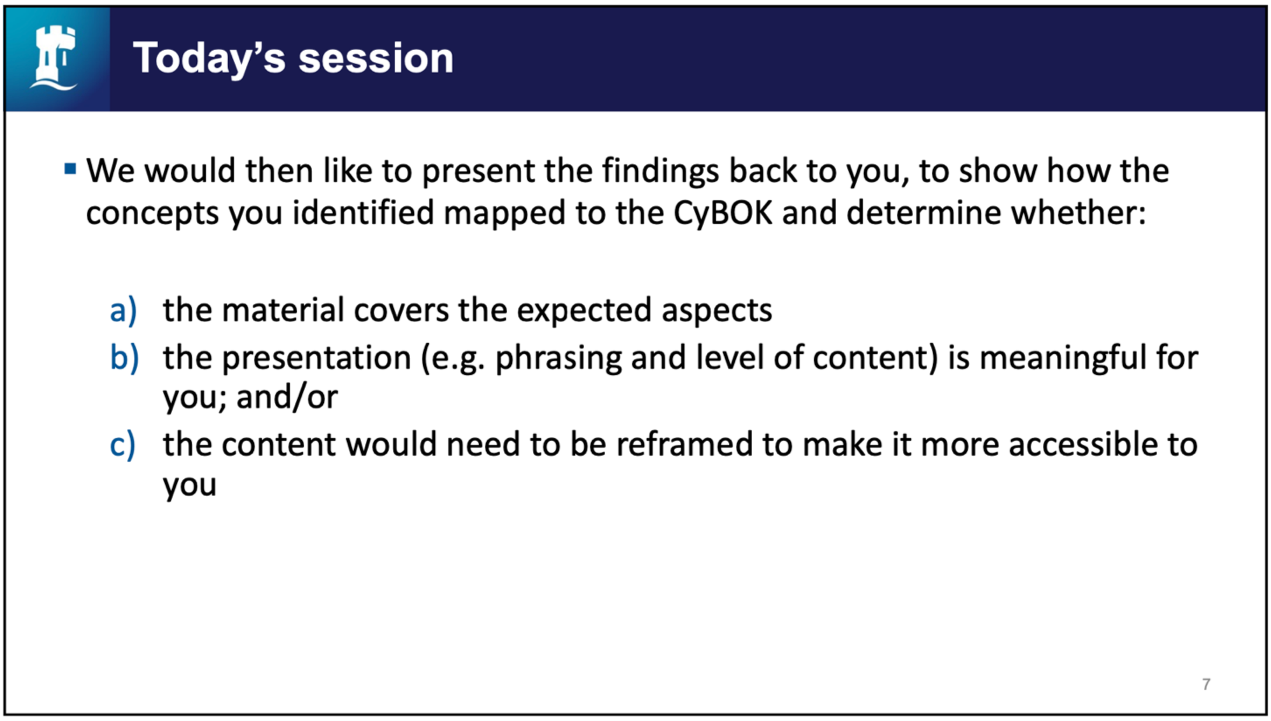
5



A reminder: The previous task

- “The activity will involve capturing key words and phrases, which we will then attempt to map against the Cyber Security Body of Knowledge (CyBOK)”
- We asked you to:
  - list any keywords or phrases that you associated with the cyber security needs of *your* organisation
  - list any *other* keywords or phrases that you associated with cyber security as a topic
  - identify any topics that you feel that your sector *contributes* to cyber security
  - Indicate your understanding of the different CyBOK Knowledge Areas and their relevance to your organisation

6



Today's session

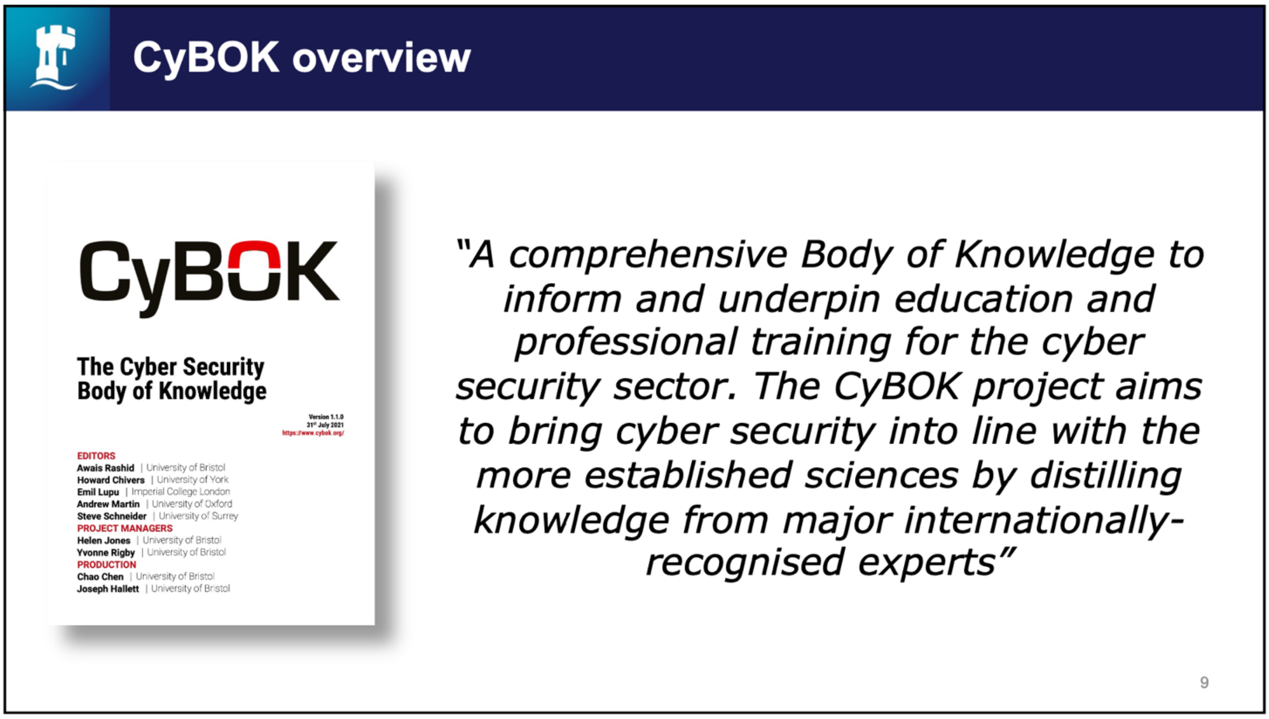
- We would then like to present the findings back to you, to show how the concepts you identified mapped to the CyBOK and determine whether:

  a) the material covers the expected aspects
  b) the presentation (e.g. phrasing and level of content) is meaningful for you; and/or
  c) the content would need to be reframed to make it more accessible to you

7

About CyBOK

8



CyBOK overview

CyBOK

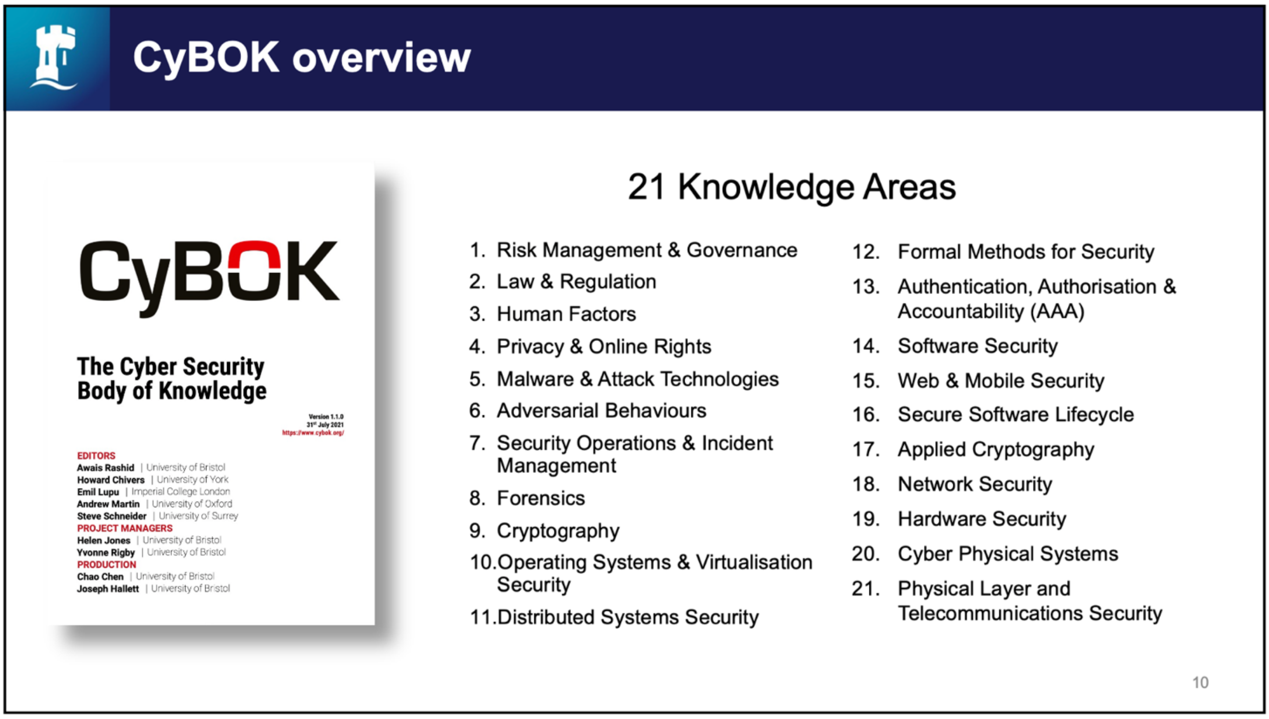
The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey
PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol
PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol

"A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector. The CyBOK project aims to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts"

9



CyBOK overview

CyBOK

The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey
PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol
PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol

21 Knowledge Areas

1. Risk Management & Governance
2. Law & Regulation
3. Human Factors
4. Privacy & Online Rights
5. Malware & Attack Technologies
6. Adversarial Behaviours
7. Security Operations & Incident Management
8. Forensics
9. Cryptography
10. Operating Systems & Virtualisation Security
11. Distributed Systems Security
12. Formal Methods for Security
13. Authentication, Authorisation & Accountability (AAA)
14. Software Security
15. Web & Mobile Security
16. Secure Software Lifecycle
17. Applied Cryptography
18. Network Security
19. Hardware Security
20. Cyber Physical Systems
21. Physical Layer and Telecommunications Security

10

CyBOK Mapping Reference

CyBOK Mapping Reference
Issue 1.3.0

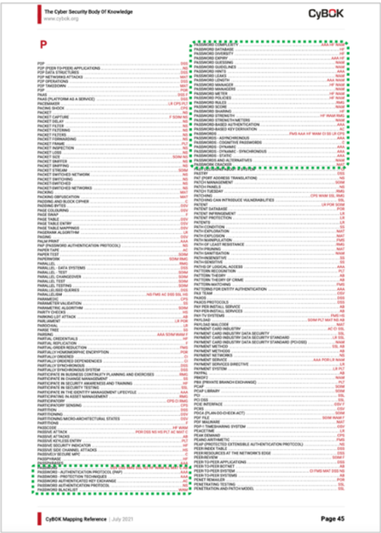
Lata Nautiyal | University of Bristol

Joseph Hallett | University of Bristol

James Clements | University of Bristol

Benjamin Shreeve | University of Bristol

Awais Rashid | University of Bristol



The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

P

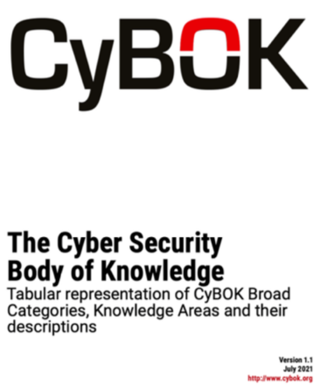
CyBOK Mapping Reference | July 2021

Page 45

70 pages of KWoPs mapped to Knowledge Areas

11

CyBOK Tabular Representation

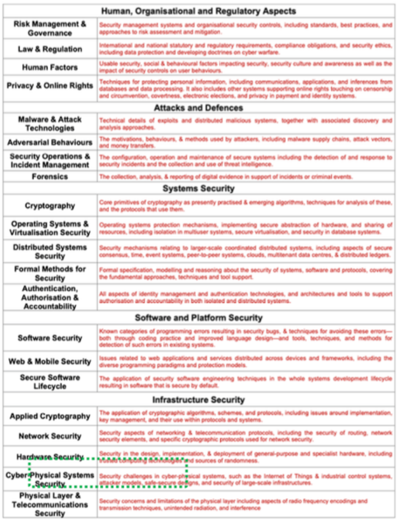


CyBOK

The Cyber Security Body of Knowledge

Tabular representation of CyBOK Broad Categories, Knowledge Areas and their descriptions

Version 1.1
July 2021
http://www.cybok.org



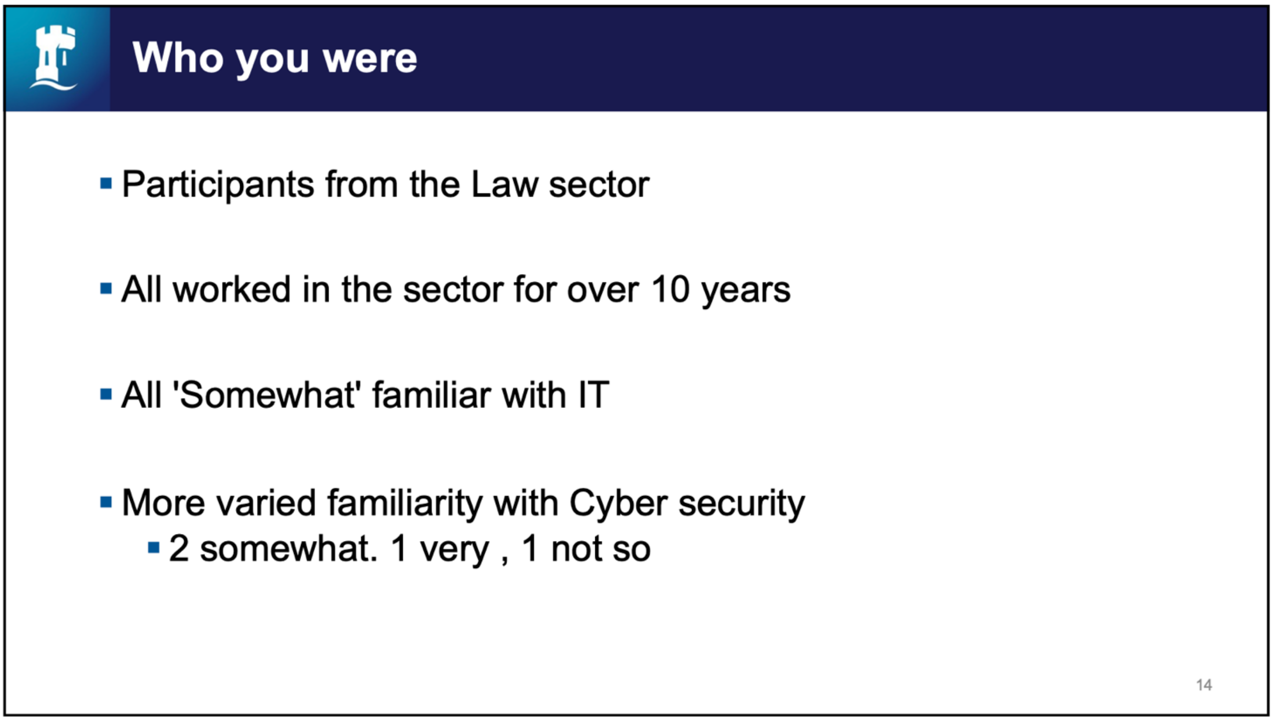
Human, Organisational and Regulatory Aspects	
Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
Attacks and Defences	
Malware & Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.
Systems Security	
Cryptography	Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers.
Formal Methods for Security	Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support.
Authentication, Authorisation & Accountability	All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.
Software and Platform Security	
Software Security	Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.
Web & Mobile Security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.
Infrastructure Security	
Applied Cryptography	The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems.
Network Security	Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.
Hardware Security	Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures.
Physical Layer & Telecommunications Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference

A summary outline of each of the Knowledge Areas

12

The Survey Findings

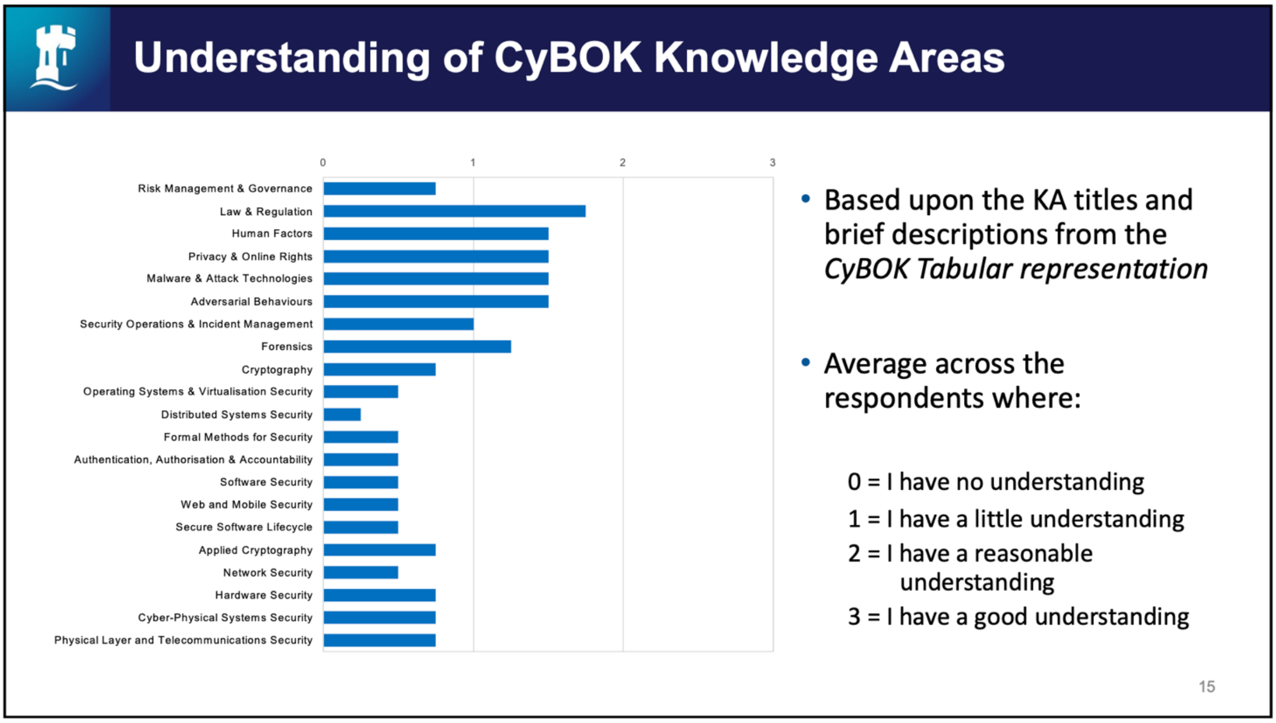
13



Who you were

- Participants from the Law sector
- All worked in the sector for over 10 years
- All 'Somewhat' familiar with IT
- More varied familiarity with Cyber security
  - 2 somewhat. 1 very , 1 not so

14

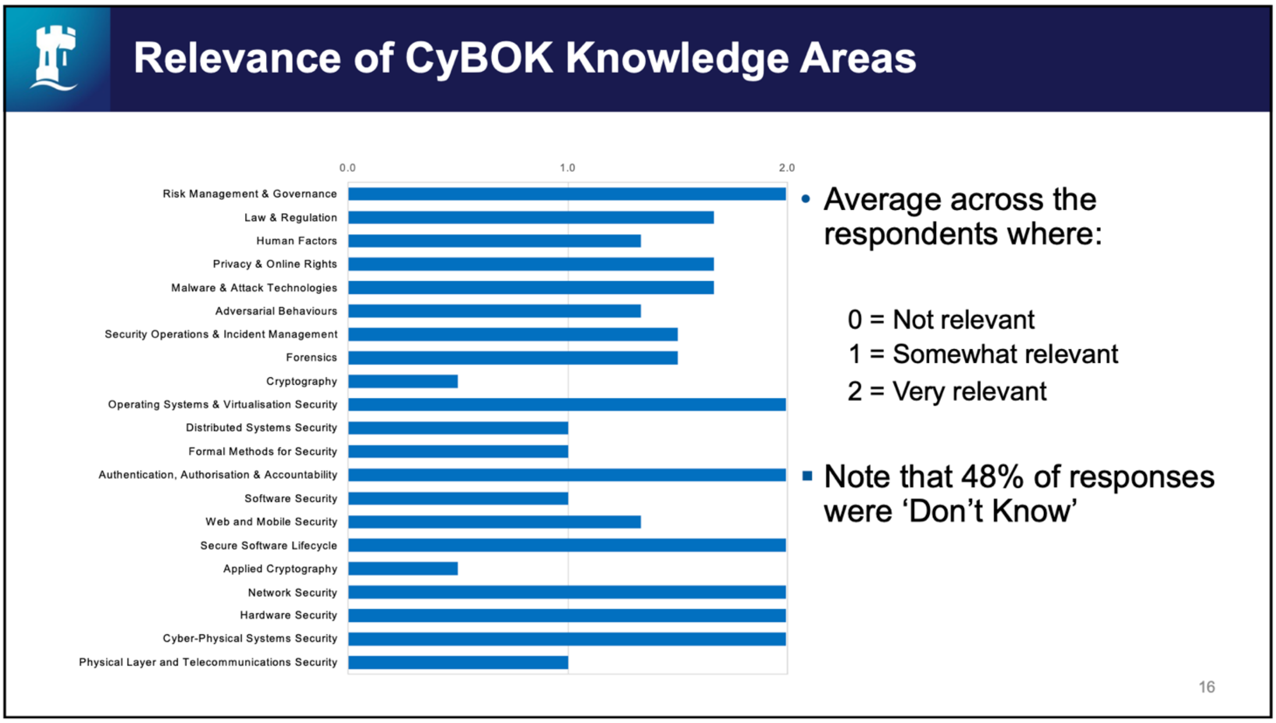


Understanding of CyBOK Knowledge Areas

- Based upon the KA titles and brief descriptions from the *CyBOK Tabular representation*
- Average across the respondents where:

0 = I have no understanding
1 = I have a little understanding
2 = I have a reasonable understanding
3 = I have a good understanding

15



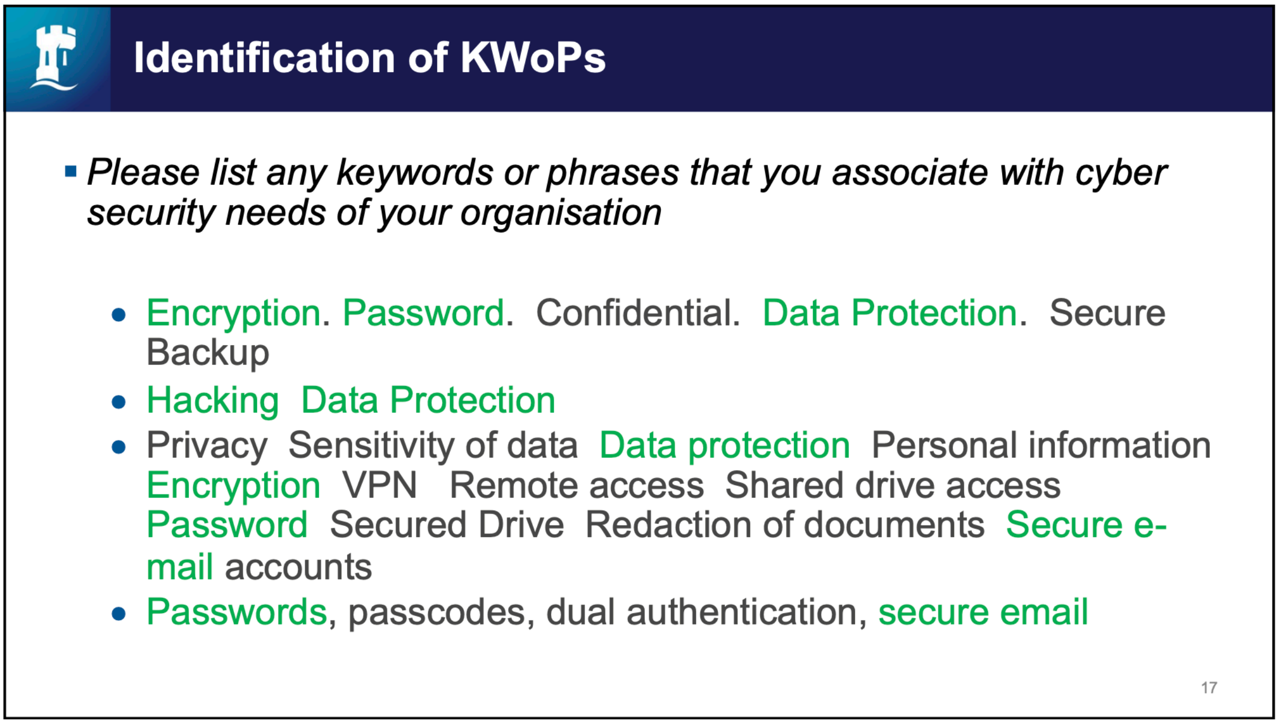
Relevance of CyBOK Knowledge Areas

- Average across the respondents where:

0 = Not relevant
1 = Somewhat relevant
2 = Very relevant

- Note that 48% of responses were ‘Don’t Know’

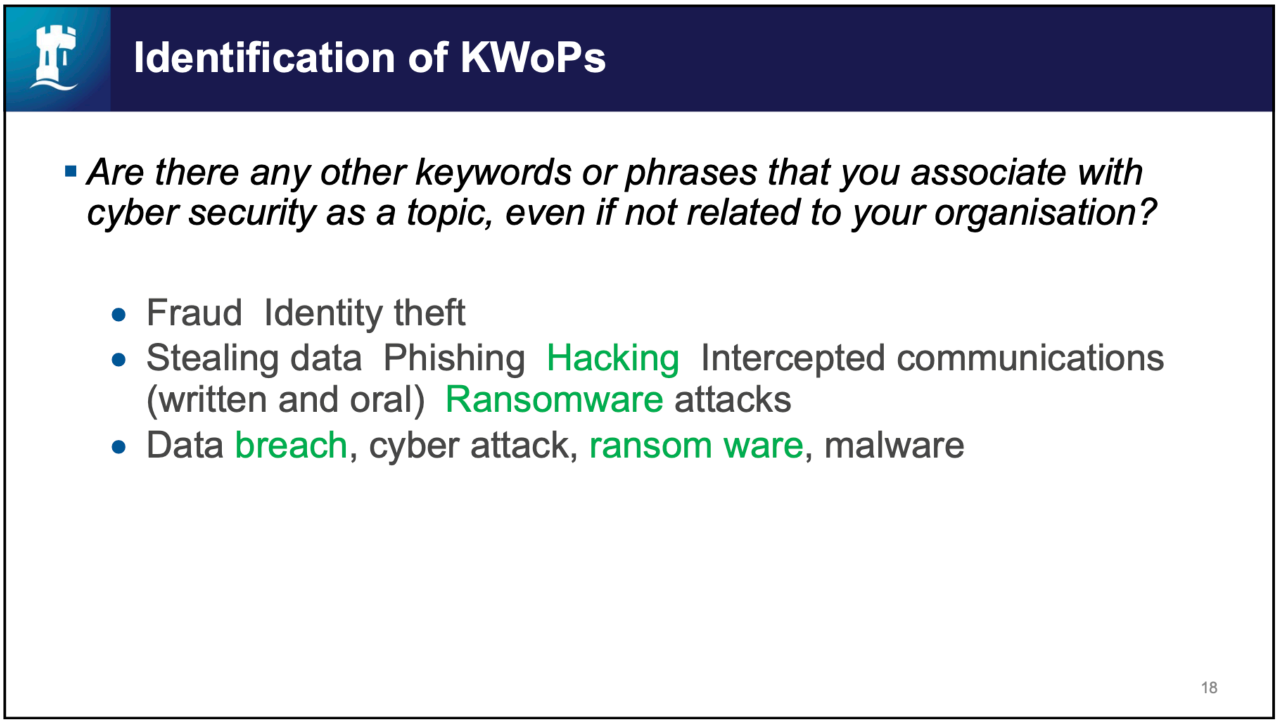
16



Identification of KWoPs

- *Please list any keywords or phrases that you associate with cyber security needs of your organisation*
  - Encryption. Password. Confidential. Data Protection. Secure Backup
  - Hacking Data Protection
  - Privacy Sensitivity of data Data protection Personal information Encryption VPN Remote access Shared drive access Password Secured Drive Redaction of documents Secure e-mail accounts
  - Passwords, passcodes, dual authentication, secure email

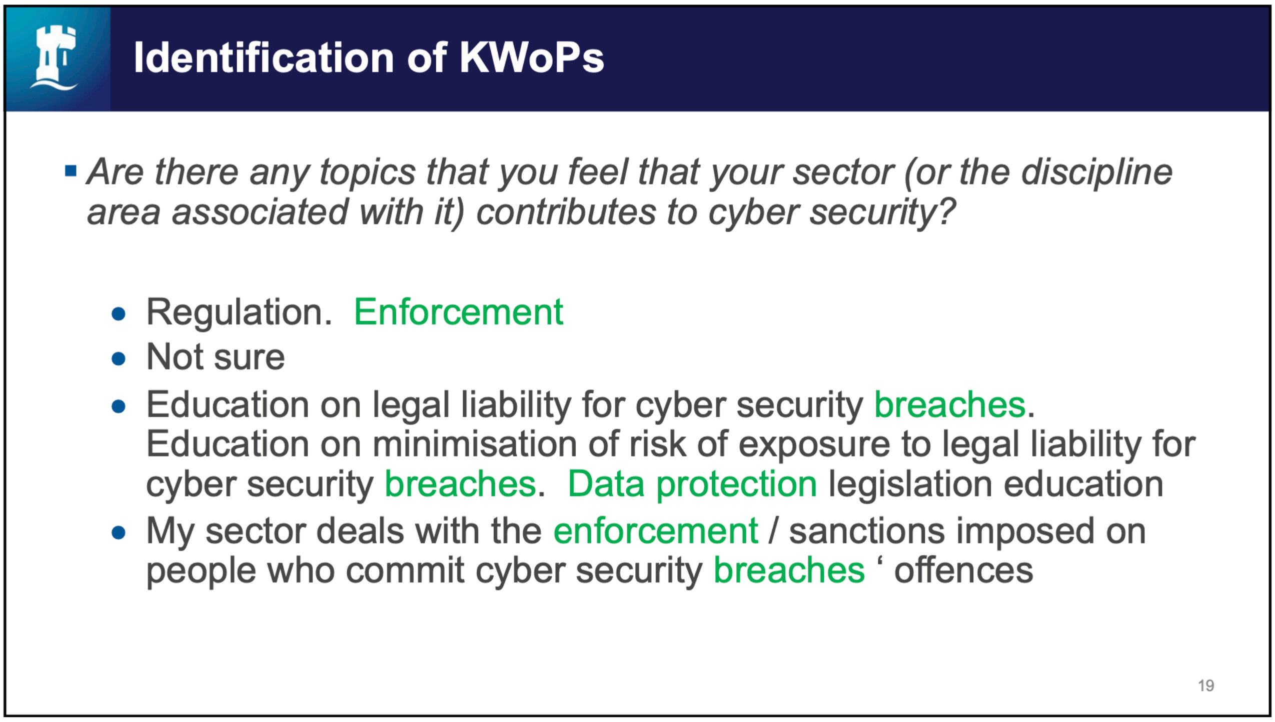
17



Identification of KWoPs

- *Are there any other keywords or phrases that you associate with cyber security as a topic, even if not related to your organisation?*
  - Fraud Identity theft
  - Stealing data Phishing Hacking Intercepted communications (written and oral) Ransomware attacks
  - Data breach, cyber attack, ransom ware, malware

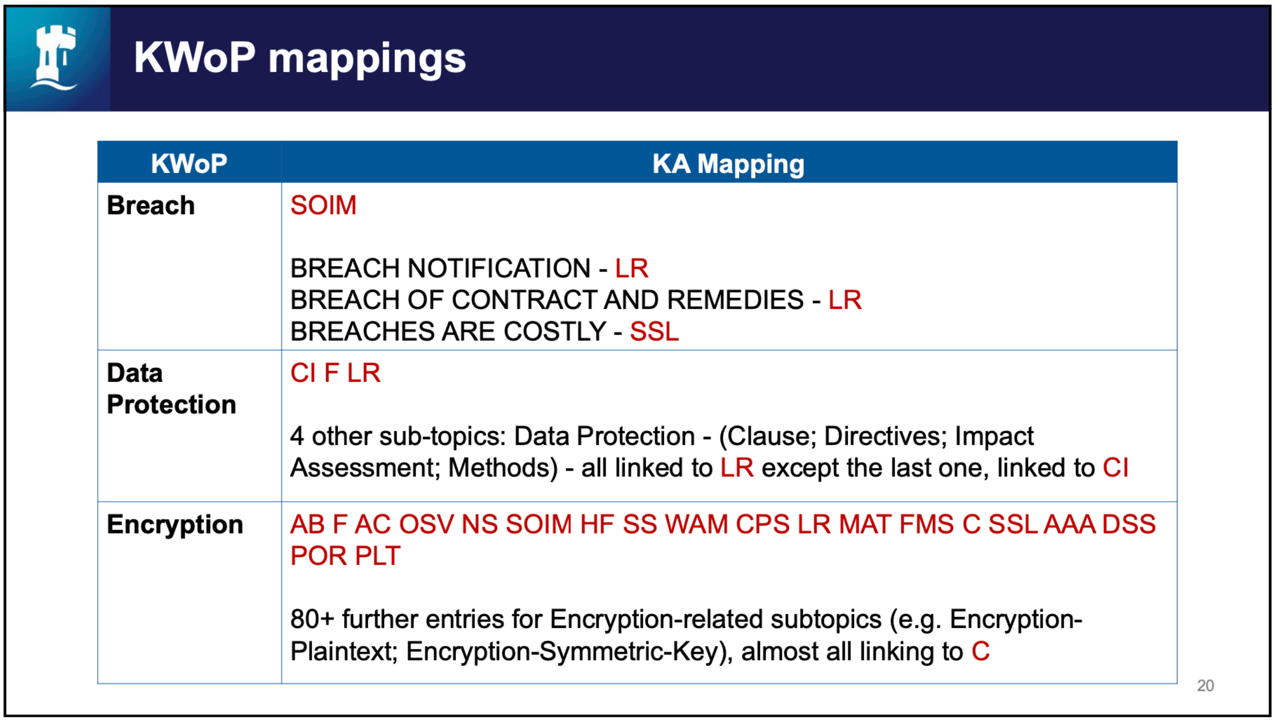
18



Identification of KWoPs

- *Are there any topics that you feel that your sector (or the discipline area associated with it) contributes to cyber security?*
  - Regulation. Enforcement
  - Not sure
  - Education on legal liability for cyber security breaches. Education on minimisation of risk of exposure to legal liability for cyber security breaches. Data protection legislation education
  - My sector deals with the enforcement / sanctions imposed on people who commit cyber security breaches ‘ offences

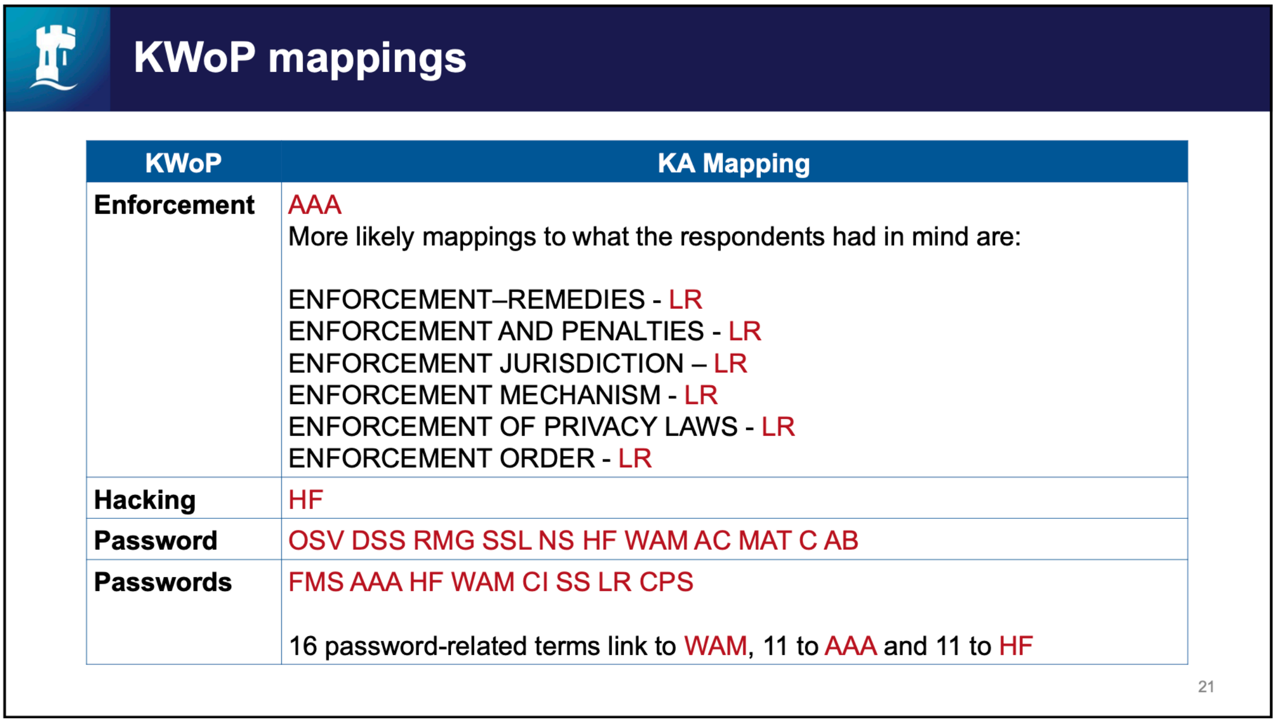
19



KWoP mappings

KWoP	KA Mapping
Breach	SOIM BREACH NOTIFICATION - LR BREACH OF CONTRACT AND REMEDIES - LR BREACHES ARE COSTLY - SSL
Data Protection	CI F LR 4 other sub-topics: Data Protection - (Clause; Directives; Impact Assessment; Methods) - all linked to LR except the last one, linked to CI
Encryption	AB F AC OSV NS SOIM HF SS WAM CPS LR MAT FMS C SSL AAA DSS POR PLT 80+ further entries for Encryption-related subtopics (e.g. Encryption-Plaintext; Encryption-Symmetric-Key), almost all linking to C

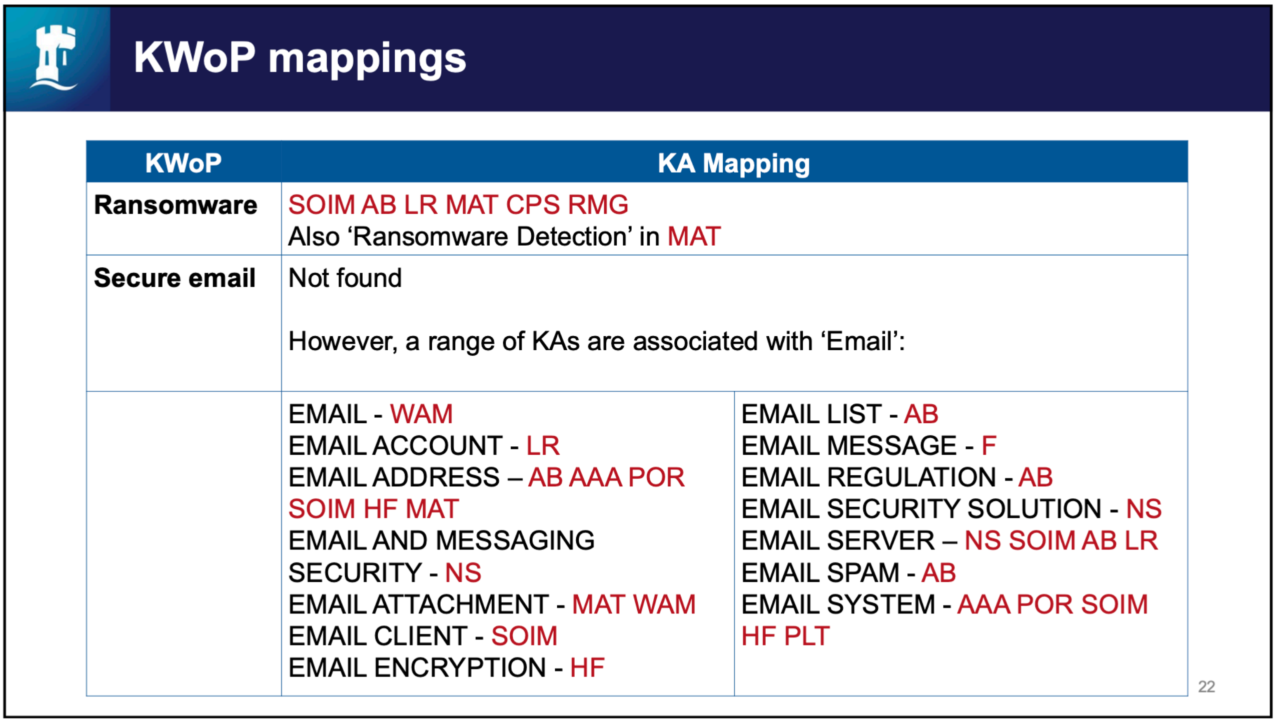
20



KWoP mappings

KWoP	KA Mapping
Enforcement	AAA More likely mappings to what the respondents had in mind are: ENFORCEMENT–REMEDIES - LR ENFORCEMENT AND PENALTIES - LR ENFORCEMENT JURISDCTION – LR ENFORCEMENT MECHANISM - LR ENFORCEMENT OF PRIVACY LAWS - LR ENFORCEMENT ORDER - LR
Hacking	HF
Password	OSV DSS RMG SSL NS HF WAM AC MAT C AB
Passwords	FMS AAA HF WAM CI SS LR CPS 16 password-related terms link to WAM, 11 to AAA and 11 to HF

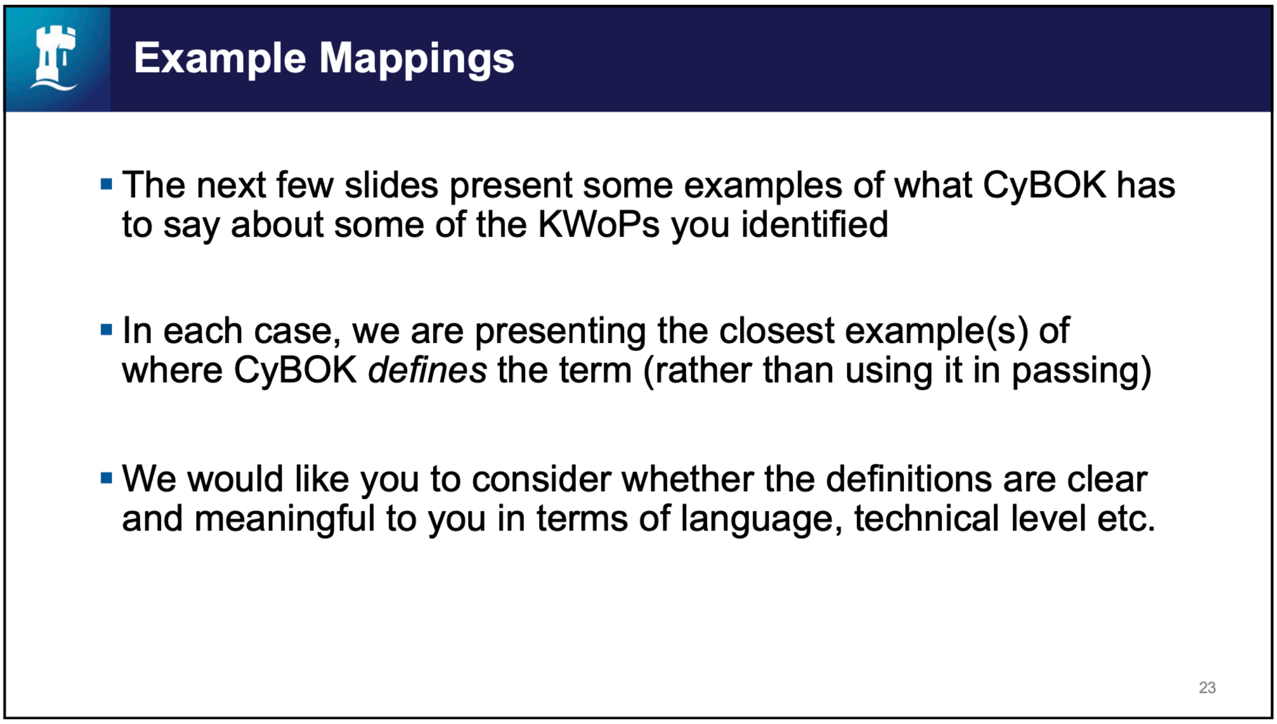
21



KWoP mappings

KWoP	KA Mapping	
Ransomware	SOIM AB LR MAT CPS RMG Also 'Ransomware Detection' in MAT	
Secure email	Not found However, a range of KAs are associated with 'Email':	
	EMAIL - WAM EMAIL ACCOUNT - LR EMAIL ADDRESS – AB AAA POR SOIM HF MAT EMAIL AND MESSAGING SECURITY - NS EMAIL ATTACHMENT - MAT WAM EMAIL CLIENT - SOIM EMAIL ENCRYPTION - HF	EMAIL LIST - AB EMAIL MESSAGE - F EMAIL REGULATION - AB EMAIL SECURITY SOLUTION - NS EMAIL SERVER – NS SOIM AB LR EMAIL SPAM - AB EMAIL SYSTEM - AAA POR SOIM HF PLT

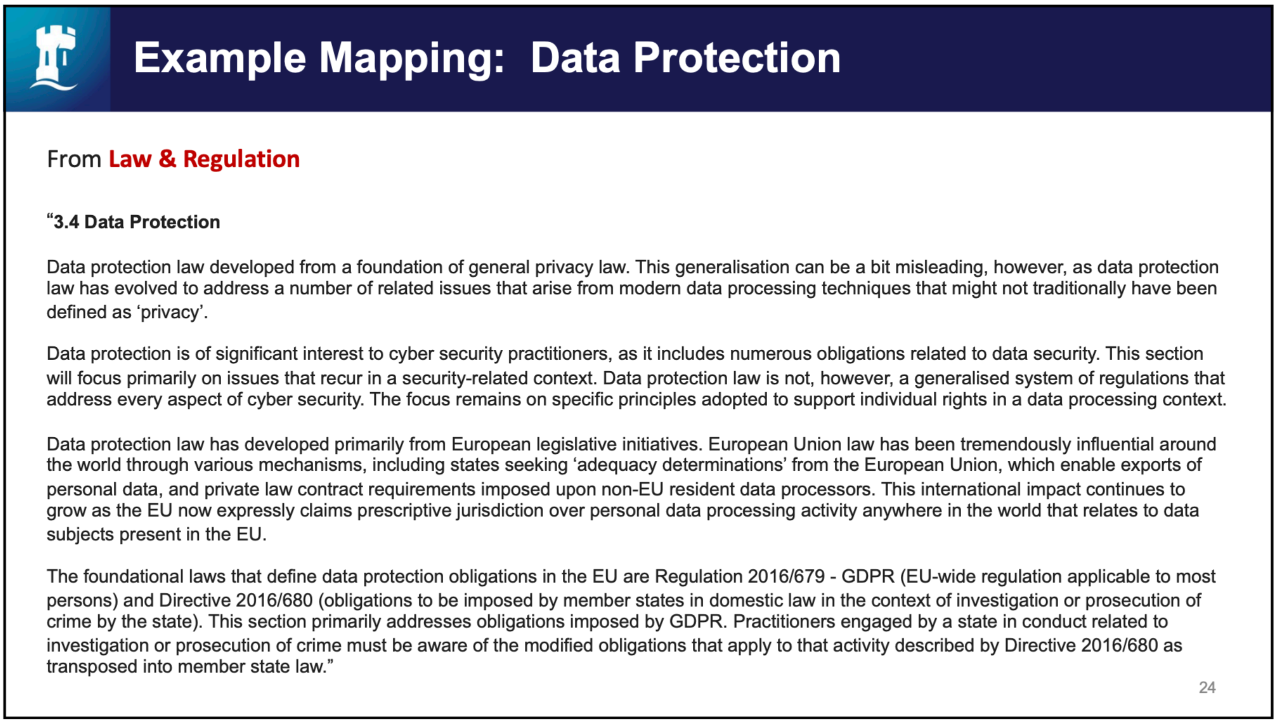
22



Example Mappings

- The next few slides present some examples of what CyBOK has to say about some of the KWoPs you identified
- In each case, we are presenting the closest example(s) of where CyBOK *defines* the term (rather than using it in passing)
- We would like you to consider whether the definitions are clear and meaningful to you in terms of language, technical level etc.

23



Example Mapping: Data Protection

From **Law & Regulation**

"**3.4 Data Protection**

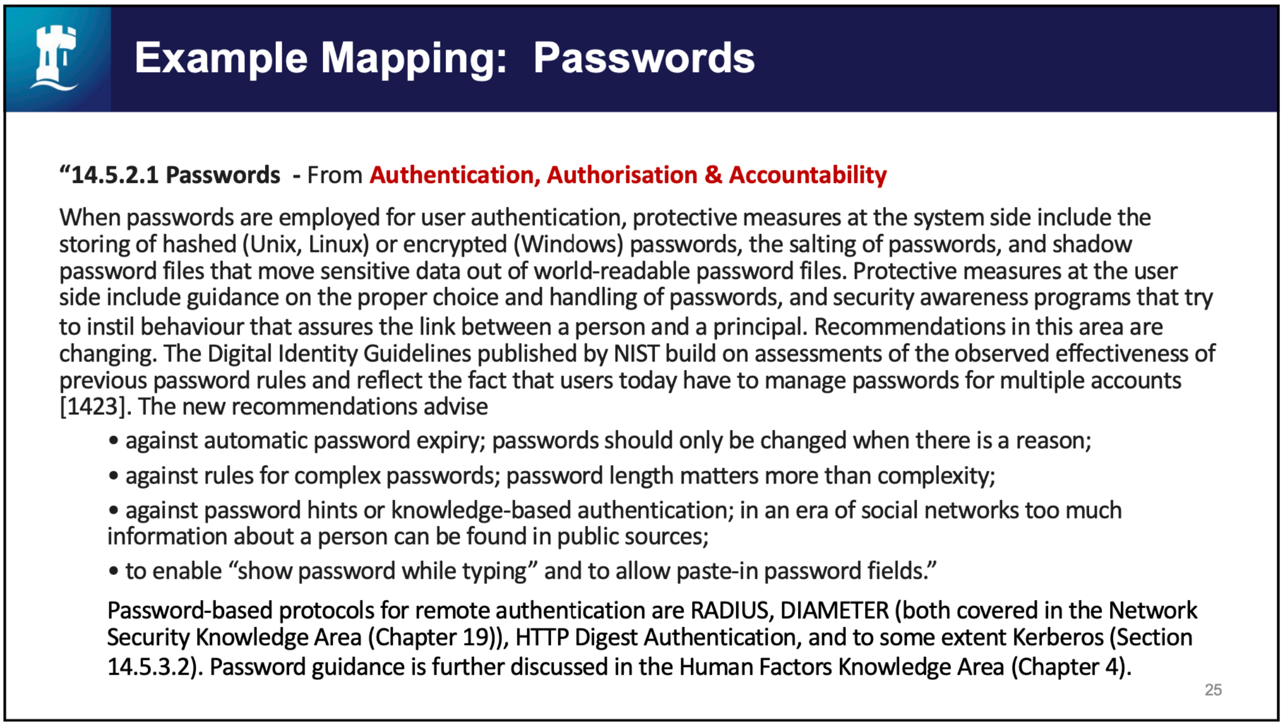
Data protection law developed from a foundation of general privacy law. This generalisation can be a bit misleading, however, as data protection law has evolved to address a number of related issues that arise from modern data processing techniques that might not traditionally have been defined as 'privacy'.

Data protection is of significant interest to cyber security practitioners, as it includes numerous obligations related to data security. This section will focus primarily on issues that recur in a security-related context. Data protection law is not, however, a generalised system of regulations that address every aspect of cyber security. The focus remains on specific principles adopted to support individual rights in a data processing context.

Data protection law has developed primarily from European legislative initiatives. European Union law has been tremendously influential around the world through various mechanisms, including states seeking 'adequacy determinations' from the European Union, which enable exports of personal data, and private law contract requirements imposed upon non-EU resident data processors. This international impact continues to grow as the EU now expressly claims prescriptive jurisdiction over personal data processing activity anywhere in the world that relates to data subjects present in the EU.

The foundational laws that define data protection obligations in the EU are Regulation 2016/679 - GDPR (EU-wide regulation applicable to most persons) and Directive 2016/680 (obligations to be imposed by member states in domestic law in the context of investigation or prosecution of crime by the state). This section primarily addresses obligations imposed by GDPR. Practitioners engaged by a state in conduct related to investigation or prosecution of crime must be aware of the modified obligations that apply to that activity described by Directive 2016/680 as transposed into member state law."

24



Example Mapping: Passwords

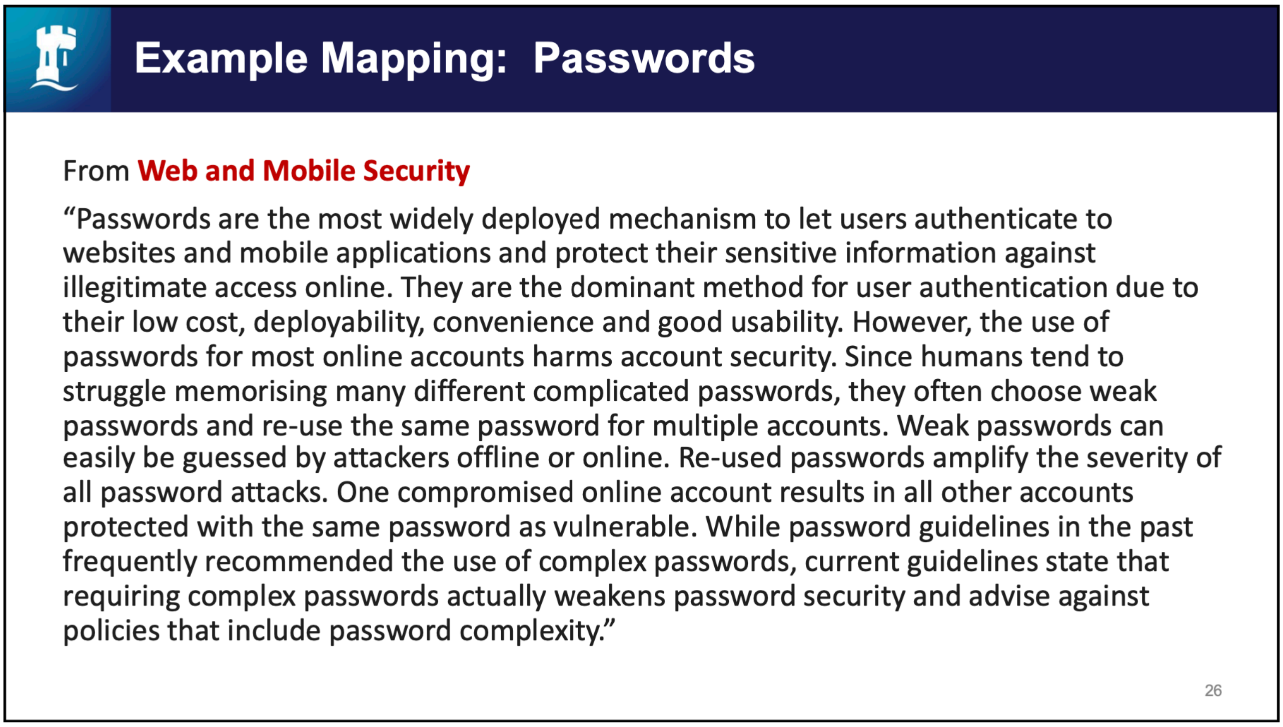
“14.5.2.1 Passwords - From **Authentication, Authorisation & Accountability**

When passwords are employed for user authentication, protective measures at the system side include the storing of hashed (Unix, Linux) or encrypted (Windows) passwords, the salting of passwords, and shadow password files that move sensitive data out of world-readable password files. Protective measures at the user side include guidance on the proper choice and handling of passwords, and security awareness programs that try to instil behaviour that assures the link between a person and a principal. Recommendations in this area are changing. The Digital Identity Guidelines published by NIST build on assessments of the observed effectiveness of previous password rules and reflect the fact that users today have to manage passwords for multiple accounts [1423]. The new recommendations advise

- against automatic password expiry; passwords should only be changed when there is a reason;
- against rules for complex passwords; password length matters more than complexity;
- against password hints or knowledge-based authentication; in an era of social networks too much information about a person can be found in public sources;
- to enable “show password while typing” and to allow paste-in password fields.”

Password-based protocols for remote authentication are RADIUS, DIAMETER (both covered in the Network Security Knowledge Area (Chapter 19)), HTTP Digest Authentication, and to some extent Kerberos (Section 14.5.3.2). Password guidance is further discussed in the Human Factors Knowledge Area (Chapter 4).

25

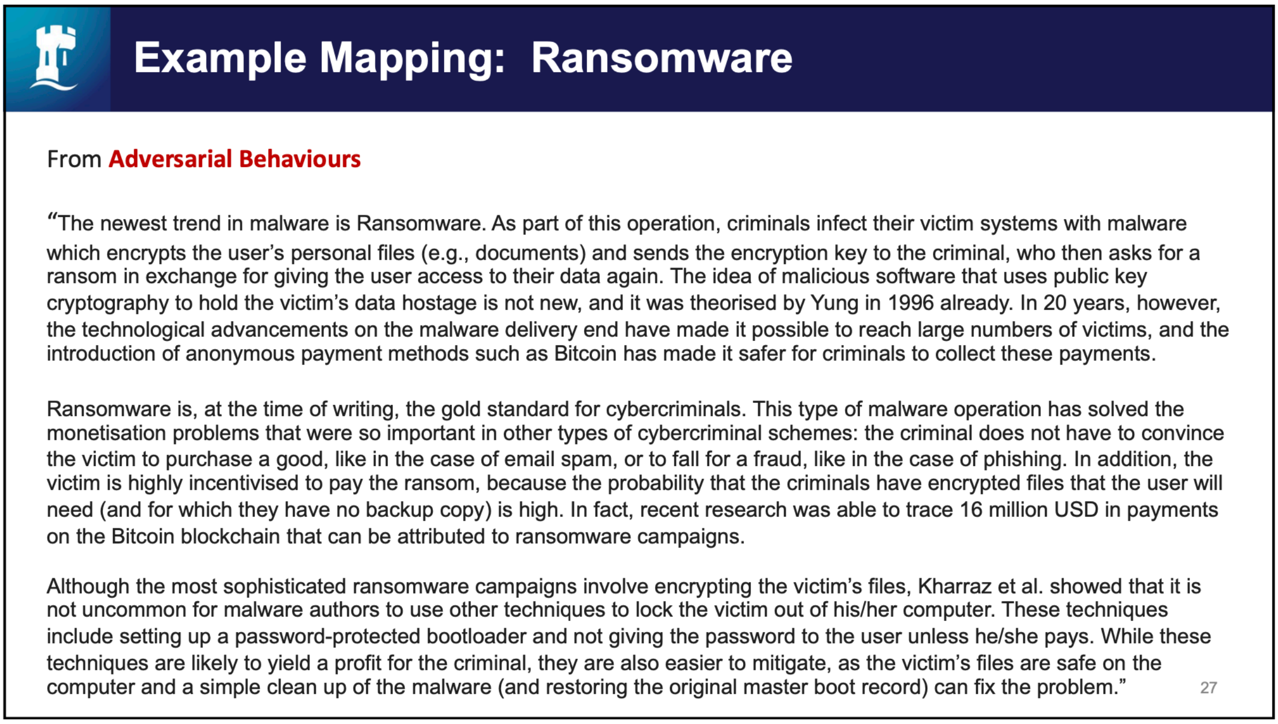


Example Mapping: Passwords

From **Web and Mobile Security**

“Passwords are the most widely deployed mechanism to let users authenticate to websites and mobile applications and protect their sensitive information against illegitimate access online. They are the dominant method for user authentication due to their low cost, deployability, convenience and good usability. However, the use of passwords for most online accounts harms account security. Since humans tend to struggle memorising many different complicated passwords, they often choose weak passwords and re-use the same password for multiple accounts. Weak passwords can easily be guessed by attackers offline or online. Re-used passwords amplify the severity of all password attacks. One compromised online account results in all other accounts protected with the same password as vulnerable. While password guidelines in the past frequently recommended the use of complex passwords, current guidelines state that requiring complex passwords actually weakens password security and advise against policies that include password complexity.”

26



Example Mapping: Ransomware

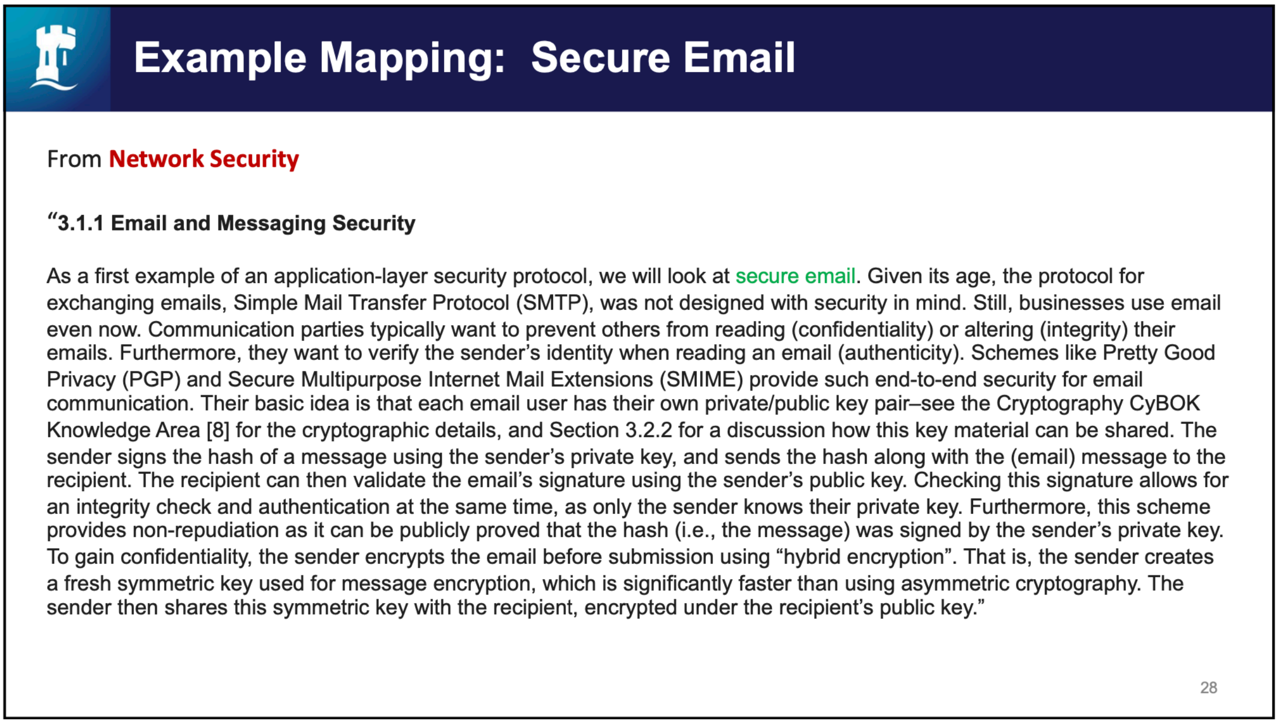
From **Adversarial Behaviours**

"The newest trend in malware is Ransomware. As part of this operation, criminals infect their victim systems with malware which encrypts the user's personal files (e.g., documents) and sends the encryption key to the criminal, who then asks for a ransom in exchange for giving the user access to their data again. The idea of malicious software that uses public key cryptography to hold the victim's data hostage is not new, and it was theorised by Yung in 1996 already. In 20 years, however, the technological advancements on the malware delivery end have made it possible to reach large numbers of victims, and the introduction of anonymous payment methods such as Bitcoin has made it safer for criminals to collect these payments.

Ransomware is, at the time of writing, the gold standard for cybercriminals. This type of malware operation has solved the monetisation problems that were so important in other types of cybercriminal schemes: the criminal does not have to convince the victim to purchase a good, like in the case of email spam, or to fall for a fraud, like in the case of phishing. In addition, the victim is highly incentivised to pay the ransom, because the probability that the criminals have encrypted files that the user will need (and for which they have no backup copy) is high. In fact, recent research was able to trace 16 million USD in payments on the Bitcoin blockchain that can be attributed to ransomware campaigns.

Although the most sophisticated ransomware campaigns involve encrypting the victim's files, Kharraz et al. showed that it is not uncommon for malware authors to use other techniques to lock the victim out of his/her computer. These techniques include setting up a password-protected bootloader and not giving the password to the user unless he/she pays. While these techniques are likely to yield a profit for the criminal, they are also easier to mitigate, as the victim's files are safe on the computer and a simple clean up of the malware (and restoring the original master boot record) can fix the problem."

27



Example Mapping: Secure Email

From **Network Security**

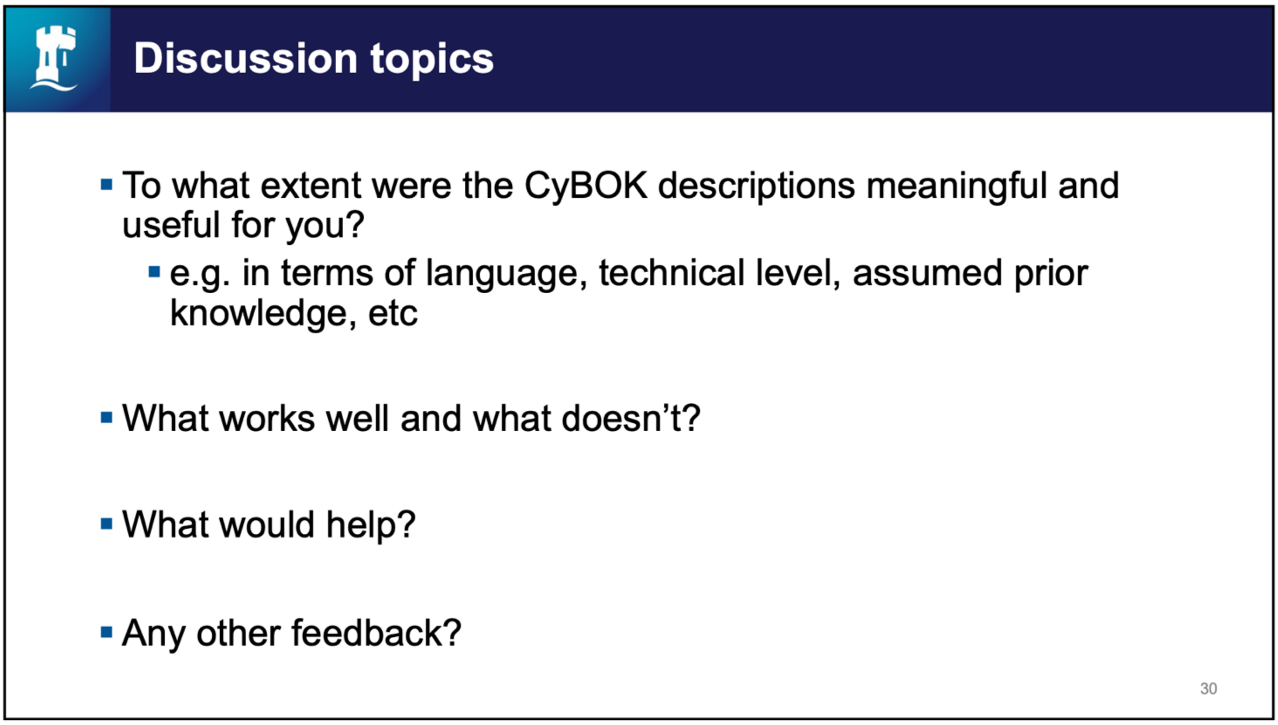
"**3.1.1 Email and Messaging Security**

As a first example of an application-layer security protocol, we will look at secure email. Given its age, the protocol for exchanging emails, Simple Mail Transfer Protocol (SMTP), was not designed with security in mind. Still, businesses use email even now. Communication parties typically want to prevent others from reading (confidentiality) or altering (integrity) their emails. Furthermore, they want to verify the sender's identity when reading an email (authenticity). Schemes like Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (SMIME) provide such end-to-end security for email communication. Their basic idea is that each email user has their own private/public key pair–see the Cryptography CyBOK Knowledge Area [8] for the cryptographic details, and Section 3.2.2 for a discussion how this key material can be shared. The sender signs the hash of a message using the sender's private key, and sends the hash along with the (email) message to the recipient. The recipient can then validate the email's signature using the sender's public key. Checking this signature allows for an integrity check and authentication at the same time, as only the sender knows their private key. Furthermore, this scheme provides non-repudiation as it can be publicly proved that the hash (i.e., the message) was signed by the sender's private key. To gain confidentiality, the sender encrypts the email before submission using "hybrid encryption". That is, the sender creates a fresh symmetric key used for message encryption, which is significantly faster than using asymmetric cryptography. The sender then shares this symmetric key with the recipient, encrypted under the recipient's public key."

28

Discussion

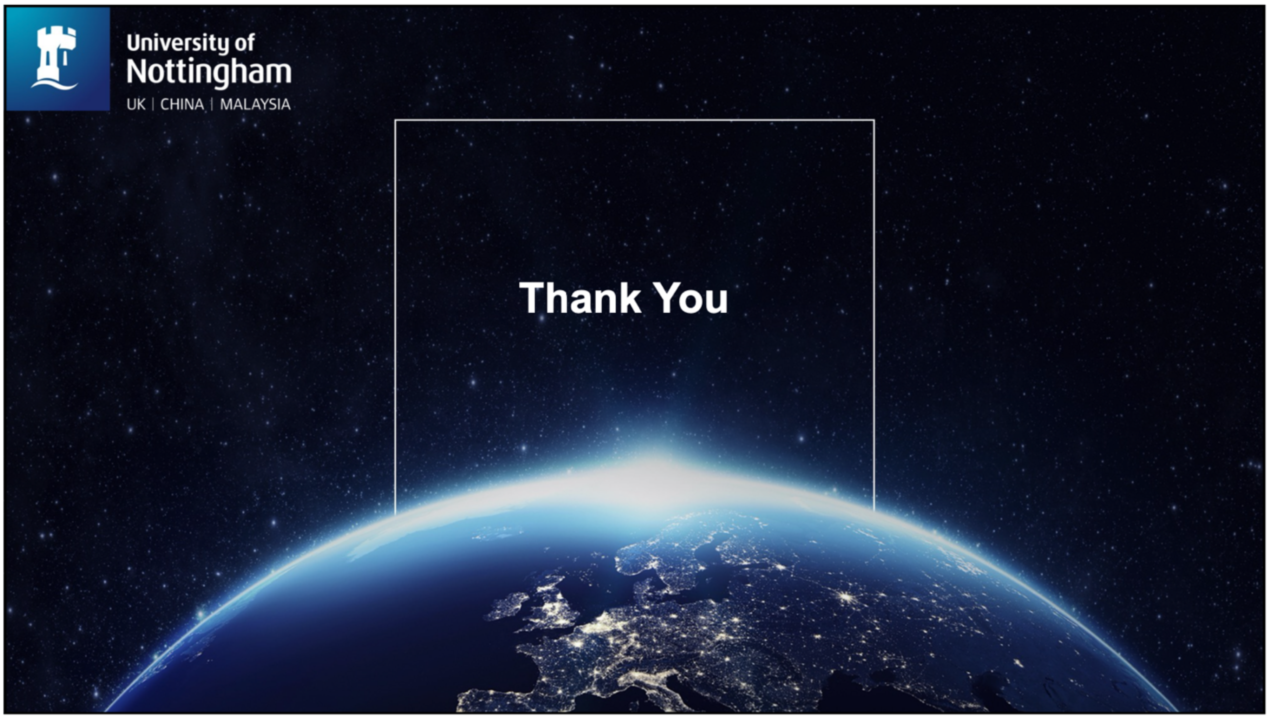
29



Discussion topics

- To what extent were the CyBOK descriptions meaningful and useful for you?
  - e.g. in terms of language, technical level, assumed prior knowledge, etc
- What works well and what doesn’t?
- What would help?
- Any other feedback?

30



University of Nottingham

UK | CHINA | MALAYSIA

Thank You

Appendix C: KWoP text excerpts

The following pages present the CyBOK excerpts that were extracted in relation to each of the identified KWoPs used in one or more of the Workshop sessions.

It will be noted that some KWoPs (e.g. ‘Denial of Service’, Passwords’, and ‘Protection’) are supported by multiple excerpts taken from different KAs, with the intention being to offer participants alternative versions and gauge their feedback on each.

KWoP	KA	Presented Excerpt
Awareness	HF	The purpose of security awareness is to catch people's attention and convince them security is worth the engagement. Given that many organisations face compliance and security fatigue, to quote Cormac Herley: More Is Not The Answer [16]: aiming a lot of communications will backfire. We need to capture people's attention, and get them to realise that (a) cyber security is relevant to them, that is, the risks are real and could affect them, and (b) there are steps they can take to reduce the risk and that they are capable of taking those steps. Crafting effective awareness messages is not an easy task for security professionals. Working with the communications specialists in an organisation can, therefore, help. They not only know how to craft messages that catch people's attention, but know how to reach different audiences via the different channels available to them, and integrate them into the overall set of communications to avoid message fatigue.
Data Protection	LR	Data protection law developed from a foundation of general privacy law. This generalisation can be a bit misleading, however, as data protection law has evolved to address a number of related issues that arise from modern data processing techniques that might not traditionally have been defined as 'privacy'. Data protection is of significant interest to cyber security practitioners, as it includes numerous obligations related to data security. This section will focus primarily on issues that recur in a security-related context. Data protection law is not, however, a generalised system of regulations that address every aspect of cyber security. The focus remains on specific principles adopted to support individual rights in a data processing context. Data protection law has developed primarily from European legislative initiatives. European Union law has been tremendously influential around the world through various mechanisms, including states seeking 'adequacy determinations' from the European Union, which enable exports of personal data, and private law contract requirements imposed upon non-EU resident data processors. This international impact continues to grow as the EU now expressly claims prescriptive jurisdiction over personal data processing activity anywhere in the world that relates to data subjects present in the EU. The foundational laws that define data protection obligations in the EU are Regulation 2016/679 - GDPR (EU-wide regulation applicable to most persons) and Directive 2016/680 (obligations to be imposed by member states in domestic law in the context of investigation or prosecution of crime by the state). This section primarily addresses obligations imposed by GDPR. Practitioners engaged by a state in conduct related to investigation or prosecution of crime must be aware of the modified obligations that apply to that activity described by Directive 2016/680 as transposed into member state law.
Denial of Service	AB	Denial of service. A feature that all Internet-connected devices have is network connectivity. A criminal can leverage the bandwidth of an infected device to perform a Distributed Denial of Service (DDoS) attack against a target. Criminals can simply use the bandwidth generated by the botnet, or leverage

		amplification attacks (i.e., network traffic generated by misconfigured network devices, or devices with poor default settings) to enhance the power of their DDoS attacks [78]. The criminals can then set up services where they offer DDoS for hire. These services are appealing for example to unscrupulous actors who want their business competitors to go offline or to online gamersonline gaming who want to knock their opponents off the Internet to win the game [79]. To hide the illicit nature of their business, these services often advertise themselves as 'stress testers', services that a Web administrator can use to test how their Web applications perform under stress [79]. In reality, however, these services do not check whether the customer purchasing a DDoS attack is actually the same person who owns the target domain.
Denial of Service	NS	Denial of Service (DoS) attacks can roughly be categorized into two categories, depending on which resources they aim to exhaust. First, in volumetric DoS attacks, adversaries aim to exhaust the network bandwidth of a victim. Amplification attacks (see Section 3.2.4) are the most dominant instance of such attacks, but also large-scale Distributed Denial of Service (DDoS) attacks from remote-controlled botnets can leverage high attack bandwidths. Attack targets are typically individual services or networks, yet can also be entire links in the upper Internet hierarchy (and their depending ASs) that become congested [133, 134]. Volumetric attacks can be mitigated most effectively when traffic is stopped as early as possible before it reaches the target network. For example, commercial so-called scrubbing services help to filter malicious network traffic before it reaches the target. Technically, scrubbing services are high-bandwidth network providers that—with the help of their customers—place themselves between the Internet and an organization's perimeter. Alternatively, attack victims can null route traffic towards certain subnetworks via BGP advertisements to drop their traffic, or use BGP FlowSpec to filter traffic at powerful edge routers. Second, in application-level DoS attacks, miscreants aim to cripple resources at the software layer. They typically aim to exhaust memory or computation resources (e.g., CPU). Here, defenses are quite application specific. For example, SYN cookies (see Section 3.2.3) and rate limiting protect TCP-based applications against connection floods. Also, CAPTCHAs may help to further distinguish between human- and or computer-generated communication, which is especially useful in the Web context.
Firewall	Gloss.	A gateway that limits access between networks in accordance with local security policy. (Source = NIST IR 7298r2).
Firewall	NS	Firewalls can be co-located with routers or implemented as specialised servers. In either case, they are gatekeepers, inspecting all incoming/outgoing traffic. Firewall systems are typically configured as bastion hosts, i.e., minimal systems hardened against attacks. They apply traffic filters based on a network's security policy and treat all network packets accordingly. The term filter is used for a set of rules configured by an administrator to inspect a packet and perform a matching action, e.g., let the packet through, drop the packet, drop and generate a notification to the sender via ICMP messages. Packets may be

		filtered according to their source and destination network addresses, protocol type (TCP, UDP, ICMP), TCP or UDP source/destination port numbers, TCP Flag bits (SYN/ACK), rules for traffic from a host or leaving the network via a particular interface and so on. Traditionally, firewalls were pure packet filters, which worked on inspecting header field only. By now, firewalls can also be stateful, i.e., they retain state information about flows and can map packets to streams. While stateful firewalls allow to monitor related traffic and can map communication to flows, this comes at the cost of maintaining (possibly lots of) state.
GDPR	LR	GDPR brought about a significant change in the territorial prescriptive jurisdiction of European data protection law [28]. GDPR, in common with its predecessor 1995 legislation, applies first to any 'processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not' (Art. 3(1)). The term 'establishment of a controller' as used in EU data protection law generally, is extraordinarily broad when compared with other commonly understood legal principles. Creating or maintaining an establishment in the territory of the EU merely means the ability to direct business affairs or activities. This definition is not restricted by the usual niceties of corporate or international tax law. A holding company in the US, for example, can be deemed to have a personal data processing establishment in the EU through the non-processing activities of its wholly owned subsidiary [29]. Thus, legal persons that have no 'permanent establishment' or 'taxable presence' in the EU for purposes of analysing direct tax liability may nonetheless be deemed to be carrying out data processing in the context of an 'establishment' in the EU for the purposes of analysing GDPR liability. GDPR now also asserts prescriptive jurisdiction over the personal data processing activities of any person, anywhere in the world, related to offering goods or services to data subjects in the EU (Art. 3(2)(a)). Prescriptive jurisdiction is believed to extend only to circumstances when the supplier volitionally offers such goods or services to data subjects in the EU.
Passwords	AAA	When passwords are employed for user authentication, protective measures at the system side include the storing of hashed (Unix, Linux) or encrypted (Windows) passwords, the salting of passwords, and shadow password files that move sensitive data out of world-readable password files. Protective measures at the user side include guidance on the proper choice and handling of passwords, and security awareness programs that try to instil behaviour that assures the link between a person and a principal. Recommendations in this area are changing. The Digital Identity Guidelines published by NIST build on assessments of the observed effectiveness of previous password rules and reflect the fact that users today have to manage passwords for multiple accounts [1423]. The new recommendations advise • against automatic password expiry; passwords should only be changed when there is a reason; • against rules for complex passwords; password length matters more than complexity;

		• against password hints or knowledge-based authentication; in an era of social networks too much information about a person can be found in public sources; • to enable “show password while typing” and to allow paste-in password fields.” Password-based protocols for remote authentication are RADIUS, DIAMETER (both covered in the Network Security Knowledge Area (Chapter 19)), HTTP Digest Authentication, and to some extent Kerberos (Section 14.5.3.2). Password guidance is further discussed in the Human Factors Knowledge Area (Chapter 4).
Passwords	WAM	Passwords are the most widely deployed mechanism to let users authenticate to websites and mobile applications and protect their sensitive information against illegitimate access online. They are the dominant method for user authentication due to their low cost, deployability, convenience and good usability. However, the use of passwords for most online accounts harms account security. Since humans tend to struggle memorising many different complicated passwords, they often choose weak passwords and re-use the same password for multiple accounts. Weak passwords can easily be guessed by attackers offline or online. Re-used passwords amplify the severity of all password attacks. One compromised online account results in all other accounts protected with the same password as vulnerable. While password guidelines in the past frequently recommended the use of complex passwords, current guidelines state that requiring complex passwords actually weakens password security and advise against policies that include password complexity.
Penetration Testing	SSL	Manual penetration testing is black box testing of a running system to simulate the actions of an attacker. Penetration testing is often performed by skilled security professionals, who can be internal to an organisation or consultants, opportunistically simulating the actions of a hacker. The objective of a penetration test is to uncover any form of vulnerability - from small implementation bugs to major design flaws resulting from coding errors, system configuration faults, design flaws or other operational deployment weaknesses. Tests should attempt both unauthorised misuse of and access to target assets and violations of the assumptions. A widely-referenced resource for structuring penetration tests is the OWASP Top 10 Most Critical Web Application Security Risks10. As such, penetration testing can find the broadest variety of vulnerabilities, although usually less efficiently compared with SAST and DAST [19]. Penetration testers can be referred to as white hat hackers or ethical hackers. In the penetration and patch model, penetration testing was the only line of security analysis prior to deploying a system.
Phishing	AB	A particular type of spam is phishing, where criminals send emails that pretend to be from genuine services (e.g., online banking, social network websites) [6]. These emails typically lure users into handing out their usernames and passwords to these services by presenting them with a believable email asking them to visit the website (e.g., to retrieve their latest account statement). By clicking on the link in the email, users are directed to a website displaying fake but realistic login pages. Once they have input their credentials, the criminals gain access to them and they will be able to later log in to those services on

		behalf of the users, potentially making money directly or selling the credentials on the black market. For the criminal, a key component to the success of phishing pages is setting up web pages that resemble the original ones as much as possible. To facilitate this task, specialised cybercriminals develop and sell so-called phishing kits [58], programmes that can be installed on a server and will produce an appropriately-looking web page for many popular services. These kits typically also provide functionalities to make it easier for the criminal to collect and keep track of the stolen credentials [58]. Another element needed by criminals to host these pages is servers under their control. Similar to spam, criminals, researchers, and practitioners are involved in an arms race to identify and blacklist phishing Web pages [59], therefore it does not make economic sense for criminals to set up their own servers. Rather, criminals often host these websites on compromised servers, for which they do not have to pay [60].
Protection	CPS	A related concept to safety is that of protection in electric power grids. These protection systems include, • Protection of Generators: when the frequency of the system is too low or too high, the generator will be automatically disconnected from the power grid to prevent permanent damage to the generator. • Under Frequency Load Shedding (UFLS): if the frequency of the power grid is too low, controlled load shedding will be activated. This disconnection of portions of the electric distribution system is done in a controlled manner, while avoiding outages in safety- critical loads like hospitals. UFLS is activated in an effort to increase the frequency of the power grid, and prevent generators from being disconnected. • Overcurrent Protection: if the current in a line is too high, a protection relay will be triggered, opening the line, and preventing damage to equipment on each side of the lines. Over/Under Voltage Protection: if the voltage of a bus is too low or too high, a voltage relay will be triggered.
Protection	HS	A set of mechanisms for ensuring that multiple processes sharing the processor, memory, or I/O devices cannot interfere, intentionally or unintentionally, with one another by reading or writing each others' data. These mechanisms also isolate the operating system from the user process" [13]. In a traditional computer architecture, usually the OS kernel is part of the Trusted Computing Base (TCB), but the rest of the software is not.
Protection	Intro	Cyber security refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.
Ransomware	AB	The newest trend in malware is Ransomware. As part of this operation, criminals infect their victim systems with malware which encrypts the user's personal files (e.g., documents) and sends the encryption key to the criminal, who then asks for a ransom in exchange for giving the user access to their data again. The idea of malicious software that uses public key cryptography to hold the victim's data hostage is not new, and it was theorised by Yung in 1996 already. In 20 years, however, the technological advancements on the malware delivery end have made it possible to reach large numbers of victims, and the

		introduction of anonymous payment methods such as Bitcoin has made it safer for criminals to collect these payments. Ransomware is, at the time of writing, the gold standard for cybercriminals. This type of malware operation has solved the monetisation problems that were so important in other types of cybercriminal schemes: the criminal does not have to convince the victim to purchase a good, like in the case of email spam, or to fall for a fraud, like in the case of phishing. In addition, the victim is highly incentivised to pay the ransom, because the probability that the criminals have encrypted files that the user will need (and for which they have no backup copy) is high. In fact, recent research was able to trace 16 million USD in payments on the Bitcoin blockchain that can be attributed to ransomware campaigns. Although the most sophisticated ransomware campaigns involve encrypting the victim’s files, Kharraz et al. showed that it is not uncommon for malware authors to use other techniques to lock the victim out of his/her computer. These techniques include setting up a password-protected bootloader and not giving the password to the user unless he/she pays. While these techniques are likely to yield a profit for the criminal, they are also easier to mitigate, as the victim’s files are safe on the computer and a simple clean up of the malware (and restoring the original master boot record) can fix the problem.
Secure Email	NS	As a first example of an application-layer security protocol, we will look at secure email. Given its age, the protocol for exchanging emails, Simple Mail Transfer Protocol (SMTP), was not designed with security in mind. Still, businesses use email even now. Communication parties typically want to prevent others from reading (confidentiality) or altering (integrity) their emails. Furthermore, they want to verify the sender’s identity when reading an email (authenticity). Schemes like Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (SMIME) provide such end-to-end security for email communication. Their basic idea is that each email user has their own private/public key pair–see the Cryptography CyBOK Knowledge Area [8] for the cryptographic details, and Section 3.2.2 for a discussion how this key material can be shared. The sender signs the hash of a message using the sender’s private key, and sends the hash along with the (email) message to the recipient. The recipient can then validate the email’s signature using the sender’s public key. Checking this signature allows for an integrity check and authentication at the same time, as only the sender knows their private key. Furthermore, this scheme provides non-repudiation as it can be publicly proved that the hash (i.e., the message) was signed by the sender’s private key. To gain confidentiality, the sender encrypts the email before submission using “hybrid encryption”. That is, the sender creates a fresh symmetric key used for message encryption, which is significantly faster than using asymmetric cryptography. The sender then shares this symmetric key with the recipient, encrypted under the recipient’s public key.
VPN	NS	Many organisations prefer their traffic to be fully encrypted as it leaves their network. For example, they may want to connect several islands of private networks owned by an organisation via the Internet. Also, employers and employees want a flexible work environment where people can work from

		home, or connect from a hotel room or an airport lounge without compromising their security. If only individual, otherwise-internal web hosts need to made available, administrators can deploy web proxies that tunnel traffic (sometimes referred to as WebVPN). In contrast, a full-fledged Virtual Private Network (VPN) connects two or more otherwise-separated networks, and not just individual hosts. There are plenty of security protocols that enable for VPNs, such as Point-to-Point Tunneling Protocol (PPTP) (deprecated), TLS (used by, e.g., OpenVPN [51]), or Secure Socket Tunneling Protocol (SSTP) […]